

Chapter 2 - Becoming a Trusted Sender B5C2-1

453

Every email marketing strategy

= subject to possibility of consumer spam complaint

Numerous legal + professional standards apply

Also, consumers expect right frequency

- right amount of content

3 authoritative benchmarks for determining if your emails = spam

1. Legal standards: CAN-SPAM act of 2003/2008 Rev.

2. Professional standards - outlined by consumer advocates + email marketing industry

3. Consumer preferences - dictated by consumers

Adhering to email professionalism

keeps emails legally compliant

improves your relationships with people who receive + open your emails

This chapter shows how to become a trusted sender
minimizing consumer spam complaints while
maximizing trust bet. your business + your
existing + future email list subscribers

I. Complying with the Spam Laws

454

CAN-SPAM act of 2003 - Controlling the Assault
of Non-Solicited Pornography + Marketing

Summary: www.ftc.gov/bcp/online/edcams/spam/rules.htm

2008 revisions: www.ftc.gov/os/2008/05/R411008frn.pdf

This section broadens your understanding of industry ^{practices}

But - consult your own attorney for more info

A. Determining which emails have to comply

- (454) CAN-SPAM act applies to commercial emails
 ≠ transactional or relationship messages
1. Commercial email contains advertisement, promotion or content from business Web site
 2. Transactional or relationship email - all else!
- Understand that all emails sent in name of your bus
 = can be construed by recipient as commercial.
- Best practice = keep all emails legally compliant
- 2008 Revisions specify that emails forwarded to others
 by a recipient may be subject to CAN-SPAM requirements
- Talk to ESP - make sure forwarded emails = compliant

B. Collecting email addresses legally

- 455 CAN-SPAM act makes certain types of email collection
 ≠ legal & requires permission from subscribers ^{email list}
 before you send certain types of content
 = affirmative consent (+ permission)
- Potentially illegal collection practices
 ≠ always easy to spot
- Best practice - make sure you have explicit permission
1. Never purchase email list from company that
 allow you to keep email addresses as a data file
 = easily bought & sold & those with explicit permission
 = too valuable to sell!
 2. Never collect email addresses from Websites &
 online directories -
 ≠ have affirmative consent

- (455)
3. Don't use an email collection service unless it gets confirmed permission of every subscriber
 4. Don't borrow an email list from another business + don't send email to another's list + explicitly opted-in to receive your emails
 5. Don't rent an email list unless = certain their practices = legally compliant

C. Including requested content in your emails

1. Provide a way for subscribers to opt out
Requirement = remove within 10 days
+ add back w/ explicit permission
It's + legal to charge someone to opt out or to ask for any information except email address + opt out preferences
Process must be accomplished by replying to replying to a single email or visiting a single Web page

ESPs can provide an opt-out link

- 456
2. Make sure your email includes your physical address
Can use po box as legitimate bus. address
 3. Make sure email header info clearly identifies your business and + mislead audience in anyway
From line
Subject line
email address
 4. Make sure your email's subject line + misleading
 5. Make sure email clearly states = solicitation unless have permission of all on list to send your solicitations (see later parts of chapter)

457

6. Make sure email complies with ^{material} any applicable guidelines for sexually-oriented subject line must comply & clearly states that content = adult in nature
 ≠ explicit in way you describe content
 see: www.ftc.gov/spam

II. Asking for Permission

Collecting info w/o asking for permission causes prospective subscribers to hesitate
 Obtaining permission ensures list starts out in compliance with current laws
Take time to formulate a professional permission strategy before embarking on email collection tactics
 Can reward you with loyal subscribers who love to open, read & take action on your emails

A. Deciding on a Permission level

Put yourself in subscriber's shoes - to assess level of permission necessary to meet ind. expectations
 Each type = 2-way motion level of consent

- 1) You should be able to attest to each subscriber's ^{email}
- 2) Subscriber should feel they authorized you to send

This 2-way permission comes in 3 basic levels

1. Implied permission = when someone shares email address in course of normal bus. commun.
 Implies that purpose of giving you E. address = to receive emails
 ≠ recommended as best practice

Ex. form includes email

Risk - subscriber may feel violated

458

≠ take much extra effort to move from implicit permission to a higher standard

Ex. Add language: "By sharing your email address you'll receive... along with monthly updates to which you can safely unsubscribe any time."

2. Explicit permission = when you include text or language disclosing how you plan to use prospective subscriber's email address

Ex. visitor who clicks Sign Up to Receive Newsletter & then clicks link on next pg. to submit info

Ex. Prospective subscribers contact you & ask to be added

Process ≠ have to be lengthy or complicated

Examples of explicit permission:

a. Verbal - when someone shares his email address via a business card, ask: "Is it alright if I send you our monthly newsletter?"

b. Written - if subscriber writes you and you respond: "BTW, may I add you to our email list so you can receive our monthly newsletter?"

c. Physical - some users physically add their email address to a guest book or

sign up or a paper form, could post sign next to it: "Thank you for giving us permission to send you... We promise never to share it with others outside company without your permission."

(458)

d. Incidental - sometimes you ask for explicit permission in context of a transaction related to your email info.

Ex. to give shoppers ability to receive cross-promotions by selecting checkbox during check out process

Text describing checkbox could read:

"select this checkbox to receive periodic promotions that enhance the value of your purchase. Be sure that default setting = unchecked!"

459

3. Confirmed permission - when someone implicitly or explicitly subscribes to email list + you respond to subscriber with email requiring subscriber to confirm his interest by reading your intended usage + then clicking a confirmation link

If reader $\neq$ confirm, address $\neq$ added to list

460

This form = most professional but most difficult for subscribers to understand so, only appropriate if:

a. you send sensitive info

b. Your subscribers tend to forget they signed up

c. You want physical record of their authorization

Generally $\rightarrow$ low response rates! So, may lose potential subscribers

Tradeoff - those who do confirm permission = more likely to receive & open your email

459 Aside - Don't Mix Your List Messages

Ex. Don't put travel agent newsletter signup at your restaurant - may confuse them as to what they'll receive

B. Inheriting a list: Getting permission after the fact

460 Ex. You purchased existing bus. + inherited email list w/ knowing source of E. addresses on list

Ex. Your list contains E. addresses collected over time + you + identify each type of associated permissions

Ex. You purchased a list or built your list with low permission standards before reading this + now you wonder if list = useless

Sending emails to a permission-less list may violate current CAN-SPAM laws

+ = likely to -> high # of complaints from recipients

Follow these steps to determine permission status:

1. Sort your list by source

if source + imply a 2-way bus. relationship

+ recipient likely + recognizing your E. address - discard the email address or

set aside contact info to ask for permission

2. Sources can be order forms,
email correspondence,
guest books,
business cards,

purchase lists

Inherited lists rarely detail the source as a file in a database, or a note on back of bus. cards

(461)

- Always discard purchased lists ($\neq$ permission-based)
2. Sort your list by date - discard any addresses of customers who $\neq$ make purchase in over a yr.
Only retain if name = recognized as current cust.
 3. Check your list visually - discard any addresses that begin with ambiguous names or = part of a distribution list
inc. Webmaster@ and Info@.
Distribution list = single email addresses that forwards email to multiple addresses.
 $\neq$ possible to tell if addresses = permission-based
 4. Sort the rest of the list by category
at this pt., consider using diff. messaging depending on your relationship to person who owns email list
Ex. Proceed more cautiously $\bar{c}$ prospects vs. customers who purchase several times
 5. Confirm permission to send email
If email list passes preceding 4 steps + people who own email addresses on list will recognize your business + your relationship to them personally
contact them to confirm permission
 - a. If you have small list - confirmation confirmed $\bar{c}$ phone call or email $\bar{c}$ ^{confirmation} link
 - b. If can't contact people personally - send a professionally written confirmation email

462

B5C2-9

Verifying permission for old outdated questionable list
- frustrating even if follow all these steps
People change addresses frequently
Database may not inc. info you need

If process = too labor intensive, } bite the bullet
proves to be impossible or if } + direct list
+ make det. of state of database } or reestablish permission

If list contains other info, consider using
direct mail
phone calls
other advertising methods } to drive prospects
thru explicit
signup process

Aside - Protecting your email list

Quality list of permission-based email subscribers
segmented by interest + behavior

= something to be proud of

histo + data = assets

= represent signif. competitive advantage

Protecting your asset = as imp. as building it

Don't violate the trust of your subscribers!

by sharing their address with others
who don't have permission info

Don't abuse subscribers by sending + ask for
or for using permission as platform
to sell unrelated banner ads

As a rule - don't do anything c. list data
that + explicitly agreed to and/or
+ expected by subscribers

III. Minimizing Spam Complaints

Spam = unsolicited commercial email
consumers ≠ like receiving it!

Even if mail ≠ meet legal def. of spam,
consumers can report it as such &

∴ impede you ability to send email

Most ESP's provide easy spam button to block it

463

If your emails - perceived as spam, and
you receive too many spam complaints

ISP's will block your email server from
sending emails to their customers

As few as 2 complaints/1000 can block you
Higher % → permanent block list

Since consumers have control over spam button,

no email marketing strategy = ununique

so - keep email in line & following guidelines

A. allowing your audience to unsubscribe

CAN-SPAM requires you include a way to let
your audience unsubscribe - but

law ≠ specify which mechanisms = appropriate

You can ask subscribers to reply with their request
& then manually keep track

But - process = tedious with larger lists

Most professional practice & most automated

= use ESP to automatically & permanently remove

anyone who unsubscribes from list in 1 click

464

Most insert a one-click unsubscribe link

- 465 Providing a 1-click unsubscribe mechanism gives potential subscribers confidence when ^{subscribing}
- B. Keeping your emails from looking like spam
 Spam is in the IO of the receiver
1. I don't want it - unwanted emails = perceived as spam esp. if $\neq$ authorizing it
 2. I can't verify it - if consumers $\neq$ tell if came from legitimate source: From line
 3. I ~~don't~~ think it's too frequent - consumers perceive frequent emails as spam esp. if feel that content = irrelevant repetitive or too long
- Even if consumers $\neq$ perceive email as spam may be inclined to click spam button if
4. They can't figure out how to unsubscribe
 5. They don't trust the unsubscribe link ^{in your email}
 6. They accidentally click spam button while sorting thru their email Inbox
 7. They unintentionally include your email while clicking spam button on large group
- Keeping spam complaints to a minimum = matter of adhering to professional practices + consumer preferences
- No matter what method of accepting permission, always take prospective customer's circumstances into account

466

Minimize spam complaints over time by doing:

1. Say Thanks! Send welcome email immediately
2. Send email reminders - insert # of opt in at top of every email reminding recipient how you obtained his email address
3. Keep email frequency in line with your email content + your email list subscribers expectations
4. Reinforce branding - include logos + colors on ^{signup} forms
5. Reinforce familiarity - make From line memorable ^{familiar}
6. Send a reminder letter - remind subscribers periodically how you obtained their E address + give them links for updating preferences + ^{unsubscribe}
7. Make your email content valuable so subscribers continue to want it - see Chapter 5
8. Make signup process memorable for subscribers + clearly identify your bus. in every Email From line so audience can verify the source - see Chapter 4 ^{to optimize}
9. Ask everyone who unsubscribes from list why they don't want your email - then ^{adjust} strategy
10. Use an ESP that authenticates your emails
11. Include a description of your email content + your typical frequency in signup process
Ex. "Signing up allows you to receive our monthly email newsletter as well as periodic special offers related to our newest products."
12. Send only content your subscribers expect
13. Allow subscribers to choose their own interests
Give list of categories + mechanism for changing interests