

ANTI-SPAM FORUM 2006

Compliance Issues: views from a digital marketer

24 March 2006

Board Member Companies

Bottom Line Responsibility

- In addition to common courtesy, every instance of bad online marketing practice contributes to make to the digital marketing medium less effective
 - Each short-term “blast” contributes to long-term clutter and decline in credibility
-

No Cause for Alarm

- The new legislation is not an impediment to legitimate e-commerce and e-marketing businesses
 - It encourages industry best practices which, in turn, greatly reduce the risk of creating spam
 - Similar legislation effectively implemented in countries such as the USA and Australia
-

Are you a spammer?

- Businesses are usually in a defensive position regarding spam
 - Protecting their IT infrastructure
 - Preventing their staff productivity
 - Most businesses are NOT spammers (not part of the 200+ active spammers)
 - However, some legitimate businesses do spam intentionally or unintentionally
-

Unsolicited Bulk Email

- *Unsolicited* means that the Recipient has not granted verifiable permission for the message to be sent
 - *Bulk* means that the message is sent as part of a larger collection of messages, all having substantively identical content
 - To be spam, a message must be sent unsolicited **and** bulk
-

Best Practice – 4 Pillars

Anticipated – the recipient looks forward to hearing from them

Personal – the messages are directly related to the receiver

Relevant – the marketing is about something the recipient is interested in

Opt-out – the recipient has the option to unsubscribe at any time

Be a Responsible eMarketer

- The ADMA believes that all activities conducted by its members must protect the individual's right to control the type and content of information they receive in order to ensure that digital marketing is appealing and effective
 - Campaigns and communications should be permission-based or allow the user to opt-out of any list or campaign at any time
-

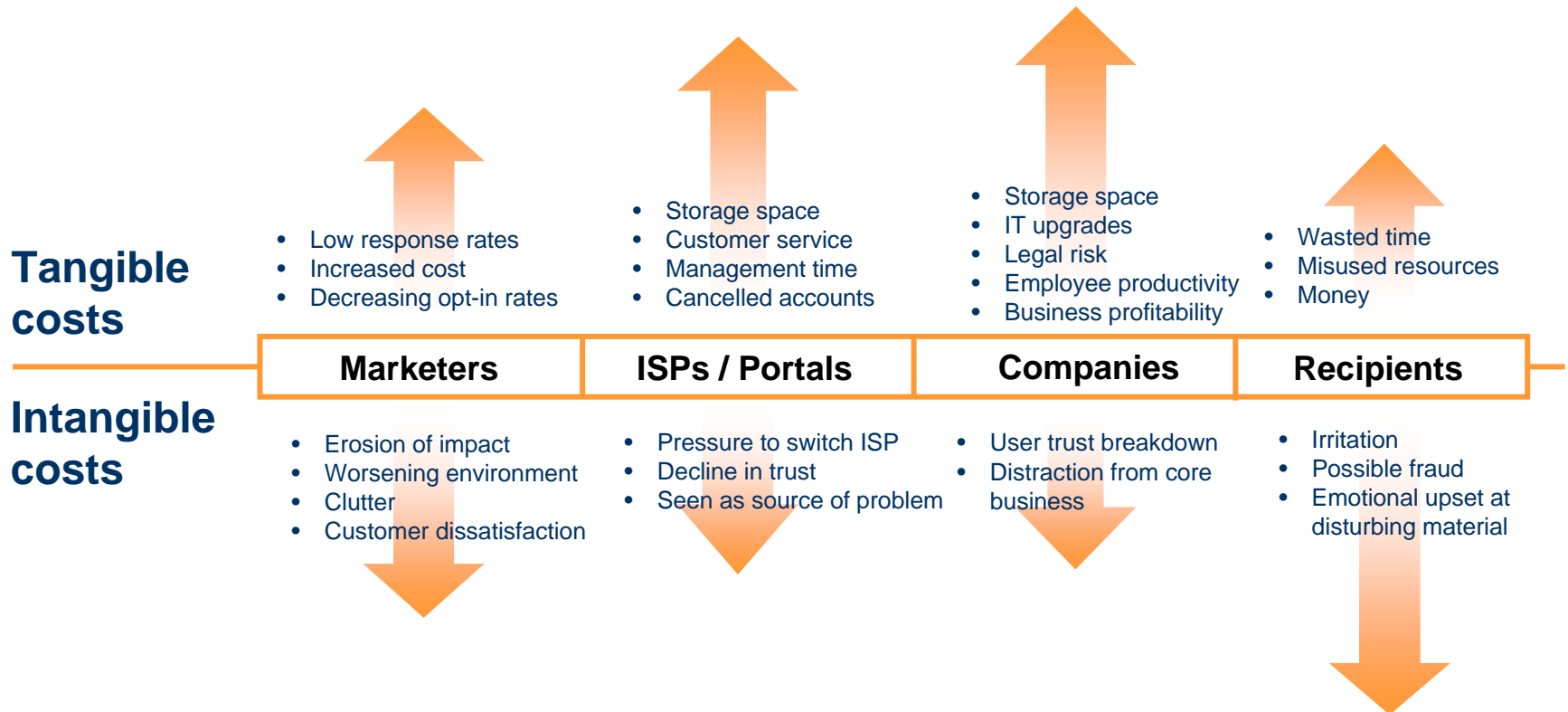
What to Focus on?

- **Notice** – state clearly why you are collecting the data and what you intend to use it for
 - **Transparency** – say what you do and do what you say
 - **Choice** – always include the “opt-out” or “unsubscribe” function
-

Guidelines for Compliance

1. Consent/permission or a prior business or personal relationship required
 2. Anticipated and relevant messages
 3. Correct sender's domain name, responsive IP address required
 4. Subject line must not be false
 5. Opt-out/Unsubscribe option required
 6. Data Privacy policy included (or link)
 7. No dictionary attacks/automatic scripts
-

Cost of non-compliance



Think...

- Are we exposing other people's email?
- Would I want to receive the message?
- Is the message easy to understand?
- Are we exposing anybody's privacy?
- Are we being interesting?
- Are we clogging people's bandwidth?

NO? Then you are in compliance and have nothing to fear!
