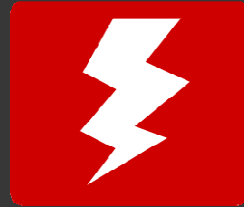


Compliance | Reputation | Advocacy



**lashback**

---

# **Global Collaborative Email Compliance and Reputation**

Enforcing the Law, Industry Standards and Best Practices

---

**Presented by:**  
**James O'Brien, Director of Marketing**

2009 © All Rights Reserved .  
Confidential. Do Not Distribute Without Permission.

- **5 Years. <30 People. 100-150 Clients.**
- **Started as UnsubSafe Toolbar Plugin**
- **Safe Unsubscribe for Consumers, Receivers & ISPs via Patent Approved Technology.**
- **Compliance Monitoring and Resolution for Advertisers, Ad Networks Publishers and ESPs through Email Compliance Monitor, UnsubMonitor BrandAlert, ListMonitor, DataSource Validator & Unsubscribe FeedBack.**
- **A Global Problem Requires a Global Solution**



- **Evolve Beyond Anti-Spam. Fraud-on-Demand Available**
- **Permission- Fake Proof of Opt-in -or- Unsubscribe- Change or Alter Identity, Brand or Offer and re-mail.**
- **US Federal Law Pre-empts State Laws (some exceptions- CA)  
Uniform System Makes Compliance Realistic and Possible.**
- **Weak Law Enforced is Better Than Strong Law Un-enforced. Over 100 CAN-SPAM Prosecutions Since January 1, 2004 is Key.**
- **Compliance Best Practices Closely Tied to Marketing BP.**
- **Positive Incentive Changes Behavior- Reputation Rewards.**
- **Associations Standards Enforcement Should be Adopted (eco)**



- **Right to Send vs. Right to Receive**
  - “With rights come responsibility”
  - Unsubscribe is the common denominator
- **Consumer Opt-Out is All in U.S.- Permission Everywhere Else.**
- **Transparency- Clear Ownership, Contact Information & Disclosure**
  - Sending IPs, Domains, From Lines, Physical Addresses
  - Authentication (Best Practice)
- **No Deception- What would a “reasonable consumer” think?**
  - (U.S. FTC Test)
- **Obligation to Monitor and Resolve Issues (U.S. FTC)**
  - Collaborative Compliance- shared liability
  - Collaborative Commerce- shared reputation

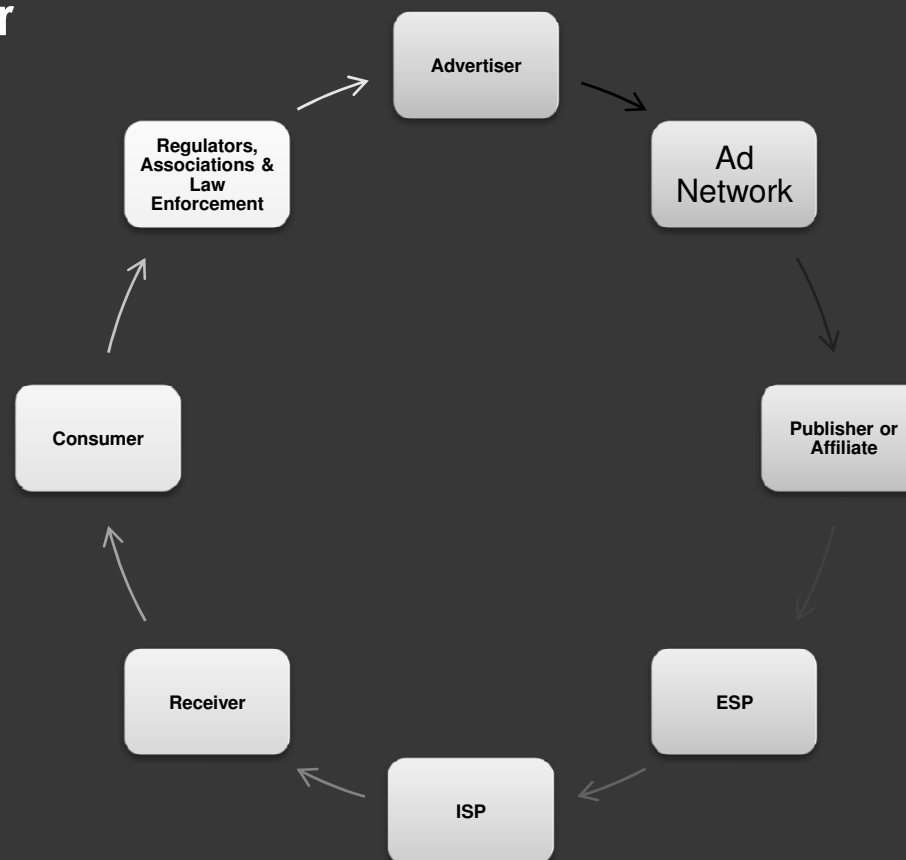
- Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (Introduced as Senate Bill 877)
- No Right of Private Action- for ISPs and Govt.
- Enforced by the U.S. Federal Trade Commission
- Electronic Mail Only- Definition is Expanding for Social for U.S.
- EU has Broader More Accurate Definition
- London Action Plan (LAP) Cross Border Cooperation is growing.

- **Who is liable?** the “Sender”
- **UK-EU** Sender is Publisher
- **US-** Sender is Advertiser in CAN-SPAM Act language
  - Principally, the advertiser whose product, service or Internet Web site is advertised in the message.
  - Each distinct line of business within a company can be considered a unique “sender” of commercial email.
  - Industry may refer to a publisher or affiliate as “sender”.
  - The term “initiate” means to originate or transmit an electronic message or to procure the origination or transmission of such message. More than one person may be considered to have initiated the message.
  - Often a list owner or email delivery service bureau is an initiator.
- **If Sender/Initiator is confusing... follow the money!**

Compliance | Reputation | Advocacy

**Who is liable? Follow the money.**  
**US= Advertiser UK= Sender**

- Where do you fit into the Email Eco-system
- Who profits?
- Is it your offer?
- Who clicks the send button?
- Do you have a hybrid business model?



## Three Types of CAN-SPAM Compliance

### Unsubscribe Compliance

- Suppression List Abuse
- Failure to Unsubscribe (10 Day Rule U.S.)
- Bad Unsubscribe Mechanism (Visible-Operable- One click- No qualifiers)

### Content Compliance

- No Postal Address (eco DE- Law U.S.)
- Relevant Subject Line
- Accurate From Line

### Sending & Data Compliance

- Send Through Open Relay
- Send to Harvested Email
- Forged Email Headers



## 1. Bad Unsubscribe Option

**Guidance:** One or more unsubscribe mechanisms must be visible and operable for minimum of 30 days after the message is sent. It is defined as a “return electronic mailing address or other Internet-based mechanism found within an email that may be used to unsubscribe from the mailing list that sent the mail.”

**Global:** Similar Requirements- Web-based encouraged.

**Best Practices:** For messages sent by affiliate networks, two opt out options should be provided - one for the advertiser and one for the publisher. These options should be clearly visible and labeled in a method that is clear to the recipient. Granular subscription management landing pages can still be offered if the premise of the new rule is followed and clearly marked global unsubscribe option is a choice. One Click unsubscribe is a best practice and follows the new rule...

**New FTC Rule:** Consumer's Only Requirement for Opt-Out is His or Her Email Address and Opt-Out Preference. No fees can be charged. No other information requested to authenticate or process opt-out. No login or other road block may be placed in the opt-out process other than sending a reply message or visiting a single unsubscribe landing page on a website to deliver opted-out email address for Suppression.



## 2. Failure to Unsubscribe or Failure to Honor

**Guidance:** Once a recipient unsubscribes, there is a ten business day period in the US to remove an email address so they do not receive any future offers. That email by law can only be used for “compliance purposes”.

**Global-** 3 or 5 Days to process consumer unsubscribe request  
Netherlands OPTA- no time limit, expectation immediate unsubscribe

“Opt-out” is the basis of CAN-SPAM’s legislative intent but is a key rule in every major email law. Permission is still a challenge to enforce, but unsubscribe is not subjective.

**Best Practices:** Scrub lists for each campaign

- Identify the list in the List-Unsubscribe header ([unsub-list2@domain.com](mailto:unsub-list2@domain.com))
- Use different List-ID headers for each list
- Use of List-Unsubscribe header can be part of an enabling system for an unsubscribe button and enhanced unsubscribe treatment when the spam or junk button is used by consumers. Other requirements including owning a good reputation, authentication, address book add is key at Microsoft, with Yahoo! and Gmail and other major ISPs using and testing variations



## 3. Suppression List Abuse

**Guidance:** A suppression list or opt-out list, is a list of email addresses that have been unsubscribed from a mailing list or group of mailing lists.

Advertisers and 3<sup>rd</sup> parties they engage are required by law to maintain and distribute a copy of their suppression lists to their partners. Cases of suppression list abuse occur when email addresses contained within the suppression file are sent email.

**Best Practices:** From a consumer perspective Suppression List Abuse is the single most critical compliance failure and can result in a significant increase in spam received and thus complaints about marketers which can hurt your reputation.

- Never distribute suppression files in raw text format
- Seed your lists and monitor – and/or – require positive ID with each use.
- Use a suppression list management service and encryption technology like MD5-Hash
- Suppression List Abuse might also be looked at as violating consumer privacy laws with the abuse of PII- Personally Identifiable Information. Consumer data privacy enforcement actions are a new trend at FTC- watch for them to increase in prevalence.

## 4. No Postal Address Provided

**Guidance:** A postal address is a physical street address or post office box address.

**Best Practice:** LashBack recommends that for messages sent by affiliate or ad networks, both the advertiser's physical address and the publisher's physical address be provided in the message.

The easier a consumer can contact your company, the more they trust your brand.

Transparency is part of the CAN-SPAM Act's Legislative Intent.

**New FTC Rule:** A Post Office Box had been verified by the FTC as a legal physical address, so long as the PO Box is registered to the business responsible for the email per U.S. Postal Regulations.

Not the law in certain countries, but an industry standard required by ECO.

## 5. Relevant 'Subject' Line

**Guidance:** A subject line is required to be relevant to the body of the message and not create false expectations on the part of a “reasonable” consumer.

**Best Practice:** Relevancy means clarity and continuity to the recipient which increases open rates and click-throughs. A worst practice would include deception which raises complaints and can violate two separate sections of FTC law. The FTC uses the “reasonable consumer test” to determine deception.

Avoid use of Re:, FWD, Proper Names, Repetitive Punctuation, CAPS.

**FTC Deceptive Advertising Policy Statement**

<http://www.ftc.gov/bcp/policystmt/ad-decept.htm>

**FTC Guide Concerning Use of the Word Free**

<http://www.ftc.gov/bcp/guides/free.htm>

## 6. Accurate 'From' Line

**Guidance:** A 'from' line is a line in the email header that specifies the sender's email address. The portion before the @ sign in the email address should contain accurate information pursuant to the offer, advertiser, or publisher.

**Best Practices:** The from line should be accurate to the body of the message and not mislead the consumer. The "friendly from" should follow the same best practices- not be inaccurate or misleading.

Never use a fictitious proper name.

Accurate "from" and relevant "subject" lines are the main variable in how a consumer treats an email. 80% of Consumers polled by the ESPC use the "Report Spam" button if they do not recognize a sender by viewing the "from" or "subject" line.\*

\* Email Sender and Provider Coalition Survey December 2006  
[http://www.espccoalition.org/ESPC Ipsos Survey Executive Summary.pdf](http://www.espccoalition.org/ESPC_Ipsos_Survey_Executive_Summary.pdf)



## 7. Forged Email Headers

**Guidance:** Forged email headers are the result of altering an email header to make it appear as though it came from somewhere or someone other than the actual source.

**Best Practices:** This point of compliance is taken very seriously by all regulators. Some laws include language wherein US Department of Justice or other law enforcement agencies could be brought in to assess the criminality of this activity beyond the a government's ability to levy civil/economic fines. Monitor email for false headers and investigate origin immediately. Contact legal representation regarding some law's requirement to report instances of forged headers when you know the identity of the party forging the header.

## 8. Send Through Open Relay

**Guidance:** An open relay is an SMTP email server that is not properly secured and relays messages from third-parties.

**Best Practices:** Typically, the owners of such servers are unaware that their server is sending these messages. This was a leading cause of UCE (Unsolicited Commercial Email) or spam as email servers default setting was "open". Inquire how your servers are protected. There is a new resurgence in corporate infrastructure being used to send illegal email .

- Eco BotNet Project



### 9. Do Not Send to Harvested Email

**Guidance:** This point of compliance covers email addresses that are systematically taken from postings or content on websites or constructed through the use of a dictionary attack.

**Best Practices:**

- Check your lists for harvested data and always know the origin of the list.
- Monitor and remove bounced email addresses
- Grouping lists by domains could show patterned attacks of common names, or generic.
- Never send to a suppression list or distribute your list to organizations marketing partners, or affiliates you suspect of abuse.

**Sending/Data Compliance Problems Will Get You Blocked or Filtered- Spamtraps, etc.**



### 10. Enforce Internal Corporate Guidelines and Best Practices

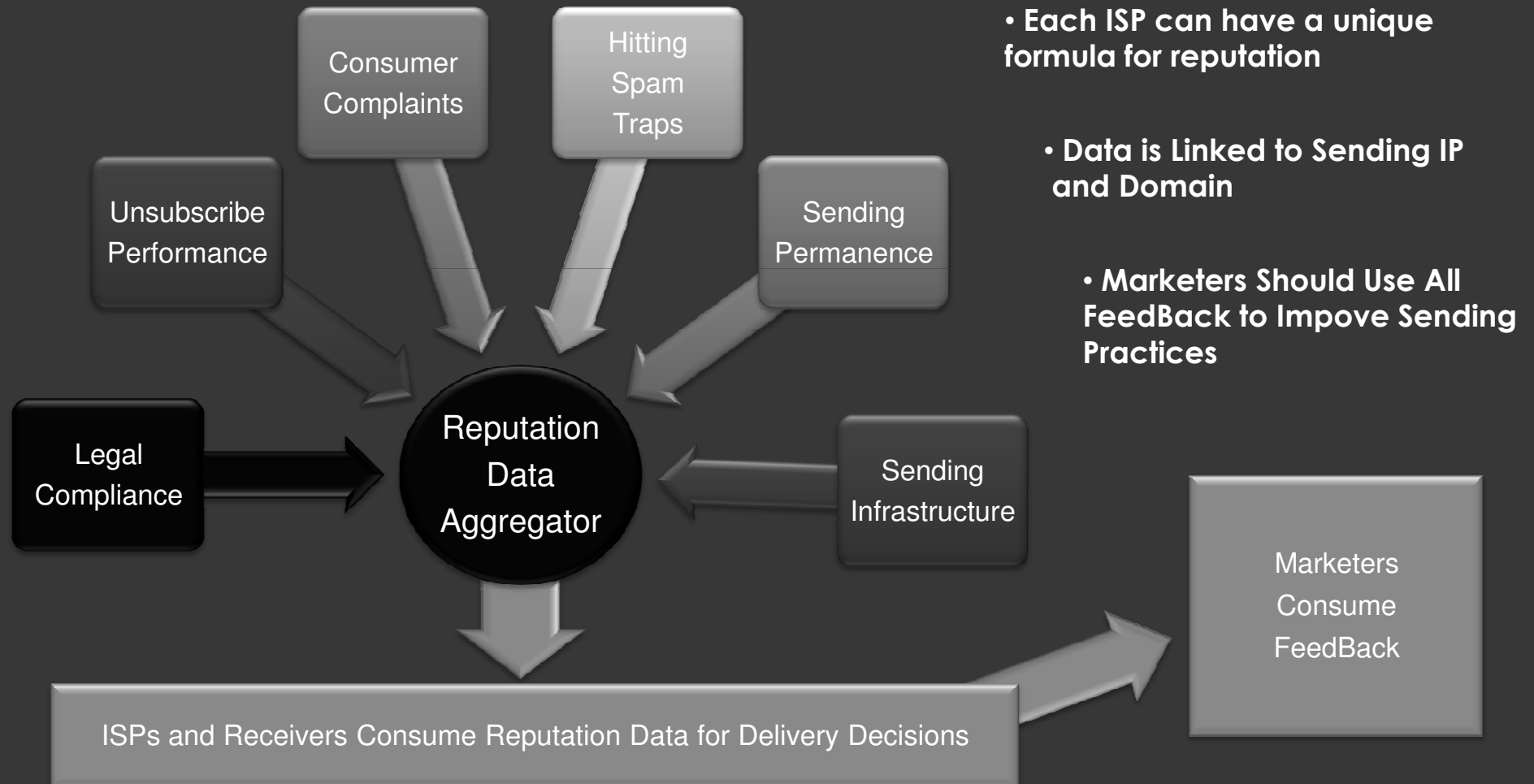
**Guidance:** Email marketers should implement custom controls which go beyond legal requirements to enforce their own corporate policies, procedures and contracts with third parties.

#### **Custom Best Practices:**

- Use of Specific, Pre-Approved Subject Lines and From Lines
- Restrict Use of Trademarks, Celebrity Images or related keywords
- Enforce Frequency and Volume Caps for Sending (ListMonitor)
- Email Brand Monitoring (BrandAlert)
- Use of List Unsubscribe Header
- Use of Authentication
- Monitor for Vertical Compliance Specific Rules: finance, education, health
- Monitor and Enforce Industry & Association Standards



# Compliance Impacts Reputation



## Benefits of Compliance

### ➤ **Decrease Liability**

- Public and private
- Identify fraud and brand abuse
- Compliance process weighs heavily under legal scrutiny

### ➤ **Protect Reputation**

- Deciding factor for inbox delivery
- Deciding factor in who works with you
- Increase brand equity

### ➤ **Increase Deliverability**

- Compliant email is first hurdle for delivery (synergy w/ common best practices)
- Identify failures or human error quickly
- Actionable feedback data improves future campaigns

### ➤ **Increase Profit**

- When email gets delivered it impacts not only gross revenue but profit per campaign

## Legal Disclaimer

LashBack, LLC. provides email compliance monitoring and educational services to advertisers, agencies, publishers, and ad networks. LashBack is not a law firm. None of the content in this presentation or any other communication from LashBack should be construed as legal advice. This presentation is intended for the sole use of LashBack clients and can be distributed by clients with permission.

LashBack is a registered trademark.




Compliance | Reputation | Advocacy



## Global Email Compliance

**Request an Email  
Compliance Seminar:**  
Call James O'Brien,  
Director of Marketing  
at 314.754.1795 or Email  
[jobrien@lashback.com](mailto:jobrien@lashback.com)

**LashBack, LLC.**   
555 Washington Ave.  
Suite 400  
St. Louis, MO U.S.A. 63101  
+1.800.434.1994

**LashBack Europe, Ltd.**   
1 Liverpool Street  
London, U.K. EC2M 7QD   
+44 (0) 7974.923.971

[www.lashback.com](http://www.lashback.com)