

## **DMA Requires Members to Adopt E-Mail Authentication Systems**

**October 17, 2005** – The Direct Marketing Association (DMA) today announced that it will begin requiring its member companies – who represent some of the nation’s largest and best-known consumer brands – to adopt e-mail authentication systems that help verify the authenticity of legitimate commercial e-mail messages.

The DMA Board of Directors voted today to require all members using e-mail for communication and transaction purposes to adopt and use identification and authentication protocols. The DMA is not requiring its members to adopt any specific authentication technology, as there are several interoperable, inexpensive and easy to implement solutions available on the market today.

“E-mail authentication protects the integrity of responsible marketers’ brands and improves the likelihood that legitimate e-mail – whether it is a marketing offer, airline ticket confirmation, or a financial statement – gets through to its intended recipient,” said DMA president and CEO John A. Greco, Jr. “Consumers can have more confidence they are getting a legitimate, valid offer from a trusted source. Marketers get fewer false positives, increased deliverability and better protection for their brands against illegal use. It’s a win-win for everybody.”

Spam, phishing and other forms of fraudulent e-mail remain an irritant to consumers and a danger because of ID thieves and others who use e-mail to perpetrate fraud. ISPs and other mailbox providers are increasingly looking to authentication as a way of reducing phishing, spoofing, and other forms of spam. Messages that do not “pass” authentication checks are much more likely to end up in a customer’s junk folder or be blocked altogether.

As efforts continue to stem the flow of phishing and spam, the DMA, along with ISPs, mailbox providers and the Federal Trade Commission, have actively supported marketplace-based authentication solutions. The DMA has created several best practice documents and white papers that help marketers understand authentication protocols and improve delivery rates for commercial e-mails. We also have numerous tips for consumers on how to guard against spam, phishing and spoofing. More information is available at [www.the-dma.org/antispam](http://www.the-dma.org/antispam).

DMA’s authentication requirement becomes the latest addition to the ethical guidelines that DMA requires its members adhere to, underscoring our commitment to the creating trust between marketers and consumers and setting the highest standards for ethical, responsible marketing practices.

### **About Authentication**

There are two major types of e-mail authentication: IP-based and cryptographic. Their goal is the same—that is, to create a master source against which to validate e-mail messages.

Authentication helps create accountability, something spammers have not had to worry about. Much of today's spam comes from senders who forge certain aspects of e-mail messages, such as the domain name in the visible "from" field.

Authentication also makes it difficult to forge IP addresses or the cryptographic signatures utilized by e-mail authentication systems. As these technologies achieve critical mass in the marketplace, someone sending an e-mail will be forced to accurately represent its origin, or else it will not be delivered. Billions of spam messages could be completely removed from circulation, meaning less clutter in e-mail boxes.

###