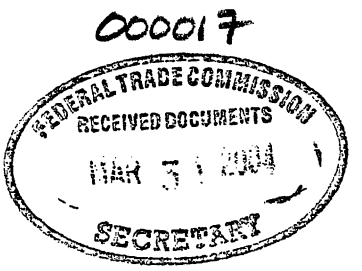
National Retail Federation
The Voice of Retail Worldwide

000017



Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

COMMENTS OF THE NATIONAL RETAIL FEDERATION

National Do Not E-Mail Registry

CAN-SPAM Act Rulemaking
FTC Project No. R411008

Mallory B. Duncan
Senior Vice President
General Counsel

Elizabeth S. Treanor
Senior Director
Government Relations Counsel

National Retail Federation
325 7th Street, N.W.
Suite 1100
Washington, D.C. 20004
(202) 783–7971

March 31, 2004

Liberty Place
325 7th Street NW, Suite 1100
Washington, DC 20004
800.NRF.HOW2 (800.673.4692)
202.783.7971 *fax* 202.737.2849
www.nrf.com

National Do Not E-Mail Registry
CAN SPAM Act Rulemaking
Comments of the National Retail Federation

The National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet and independent stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.4 million U.S. retail establishments, more than 20 million employees - about one in five American workers - and 2003 sales of $3.8 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations. NRF's larger and smaller members will be very much affected by the creation of a nationwide marketing Do Not E-mail Registry especially those who are involved in, or plan to become involved in, e-commerce.

Multichannel retailers have spent the past seven years revolutionizing the way Americans shop by giving each and every consumer greater access to a wide variety of goods and services at highly competitive prices. E-commerce has brought millions of new customers to retailers' web sites. In fact, over 40 percent of online customers are new to the retailer's entire business.[1] The Internet has also served to increase new customer traffic in brick and mortar stores after browsing online. According to the Shop.org[2] annual study for 2002, online retail sales soared to $76 billion last year, up 48

[1] *The State of Retailing Online 6.0,*2003, a Shop.org annual study of more than 130 retailers conducted by Forrester Research. Shop.org's *State of Retailing Online* 7.0 for 2003 will be available in May 2004.
[2] Shop.org is the online retailing division of NRF.

percent over 2001. The study further predicted online sales to grow another 26 percent to reach $96 billion in 2003.

In addition to growth in revenue, figures from the *State of Online Retailing* study show that online retailers in the United States are continuing their march to profitability. In 2002, 70 percent of retailers reported positive operating margins, compared with 56 percent in 2001. Collectively, online retailers broke even in sales in 2002, up from a loss of 6 percent in 2001. The 2003 Shop.org/BizRate.com *Holiday Mood Study* further found that more than half (59 percent) of retailers reported revenue growth for the 2003 online holiday season of 25 percent or higher. Almost a third (30 percent) reported revenue increases of 50 percent or more.

As multichannel retailers continue to fine-tune their online selling and marketing strategies, consumers have become more comfortable shopping online – especially with retailers that they know and trust. Online sales were expected to reach 4.5 percent of total retail sales in 2003, up from 3.6 percent in 2002.[3] It took the catalog industry 100 years to represent 4.7 percent of retail sales. It took online retailers only six years to accomplish the same feat. What has made this retail industry revolution possible is the widespread access to the Internet and e-mail by American consumers. So, while the reach of "e-tailing" is quite broad, its existence as a technology is still rather new and its patterns of use are still developing.

Many multichannel retailers routinely communicate with their customers by e-mail. Whether it is to confirm a transaction, to notify the customer of the delivery status

[3] *State of Online Retailing 6.0,*, Shop.org, 2003

of their product, or to distribute news and promotions for the customer's convenience, retailers send out millions of e-mails each and every day. The sheer breadth and expectations of the online retail customer base virtually necessitates this practice and it has proven to be an effective tool for providing customer service and building customer loyalty.

As the Internet has emerged as a primary tool of communication and commerce, commercial e-mail has come to mean different things to different people. Unfortunately, Americans open in-boxes full of offensive pornographic e-mail, get-rich schemes, and promotions for diet aids every day. However, they also receive e-mails from legitimate retailers promoting their brands, notifying customers about sales, and, often, offering free shipping on purchases. Retailers have been at the leading edge of e-mail marketing best practices. In fact, many retailers only communicate with customers who have provided them with their e-mail address and, even before the CAN-SPAM Act took effect, routinely included easy opt-outs in their marketing e-mail.

Unlike spammers, retailers have long understood that keeping their customers happy is the most essential part of building a positive long-term business relationship. That is why NRF was extensively involved in the formulation of the Federal Trade Commission' s ("the Commission") National Do Not Call list, supported the passage of legislation at the end of the 107th Congress that asked the FCC to do the same, and was actively involved in the formulation and passage of the CAN-SPAM Act. If our customers do not want to be called, e-mailed, or even sent perfume samples in their monthly billing statements, retailers want to accommodate their wishes. A satisfied

customer is a repeat customer. That being said, retailers do not want to lose an entire medium for effective e-mail marketing due to the misdeeds of spammers sending pornography and fraudulent or offensive solicitations to consumers' in-boxes.

The creation and implementation of a national do-not-email registry at this time is premature, and could have a very harmful effect on e-commerce. It would block all legitimate e-mail being sent to consumers while not serving to deter bad actors who will either flout the law or move overseas. In the end, legitimate businesses that strive to serve, not harm, their customers will become collateral damage in the war against spam. Despite NRF's support for the National Do Not Call Registry, we, and our members, continue to view e-mail as a very different medium than the telephone. E-mail is much more efficient, much less intrusive and more easily disposed of (or deleted) by the recipient than telephone calls or even traditional mail.

It should also be remembered that even the Do Not Call Registry developed over time. Congress provided the Federal Communications Commission ("FCC") with the authority, in 1991, to implement a national do not call program. The FCC weighed that option, along with several other alternatives in developing its rules. The FCC correctly determined that despite the many technological advances that had been accomplished by the end of the 1980's, the implementation of a national do not call system, at that point, would have been too cumbersome to administer when all the costs and benefits of such a program were tallied. Consequently, it adopted a more limited model that provided a level of protection beyond that which existed at the time, but that was not a model that

would have been unsustainable in practice at the time of the rulemaking. Much the same is true today.

We do not know how e-mail marketing is going to develop over the next several years. We do not know whether new software or technologies (much as caller ID was developed with respect to telephones) will soon influence the scope of the problem and the means of protection available to consumers and regulators. What we do know is that Congress provided several avenues for addressing spam in the CAN-SPAM Act. The imposition of its most extreme remedy, before we have had a chance to gauge the effectiveness of the others, is likely to impose inefficiencies and unnecessary costs on the system.

As the Commission notes, the CAN-SPAM Act took effect on January 1, 2004. In the short time that the law has been in effect it has already been credited with substantially reducing the amount of spam being generated. According to recent statistics released by America Online ("AOL"), spammers attempted to send 1.9 billion messages on March 17, 2004, down 27 percent from the 2.6 billion messages sent on February 20, 2004.[4] In its statement, AOL directly credited both an improvement in its spam filters and the CAN-SPAM Act for this decrease. This is an unprecedented reduction in spam by more than one quarter in less than three months. Furthermore, several Internet Service Providers (ISPs) have already filed lawsuits against pattern and practice spammers who have failed to meet their obligations under the Act. We at NRF believe that well thought out and targeted lawsuits against true bad actors will serve to deter others in the future.

[4] "Moneyline," *USA Today*, March 22, 2004, page B1.

Legitimate retailers send millions of pieces of e-mail every day. This is in direct correlation to the fact that they have *millions and millions* of customers who enjoy the benefits of hearing from them in this manner. In fact, e-mail was the most popular means for retailers to market to customers online during the 2003 Holiday season according to the Shop.org and BizRate.com *2003 Online Holiday Mood Study*. However, to many Spam activists and ISPs the sheer volume of communications sent out by any legitimate retailer may be deemed reason enough to label their e-mails as Spam.

In fact, retailers are fielding more and more complaints from their customers that their e-mails are not getting through. Long-time customers want to know why they didn't get their sale notices while their neighbor down the street did. Often the answer is simple: their neighbor uses a different ISP. Even more troubling is the fact that blocking acts to deflect not only marketing emails, but also e-mail that retailers are required to send customers (e.g., delay notices under the FTC Mail and Phone Rule) and e-mail customers expect to receive (e.g., order confirmations). Recent statistics compiled by Assurance Systems in the fourth quarter of 2002 show that fully 15 percent of permission-based e-mail never gets through to subscribers of the largest ISPs.[5]

Despite this fervent blocking, it is clear that the average consumer views the e-mail that they receive from the retail industry very favorably. According to a survey conducted by Bigfoot Interactive and NOP World Research[6] in February of this year, 90 percent of consumers eighteen years and older who receive permission-based e-mail and 83 percent of consumers who receive unsolicited e-mail from retailers are very satisfied with the retailer. In fact, 91 percent of the participants who receive permission-based

[5] "Fourth Quarter 2002, E-mail Blocking and Filtering Report," Return Path Assurance Systems, February, 2003.
[6] "Retailer's E-mail Achievements," *E-Marketer,* March 10, 2004.

e-mail are more likely to buy products from the retailer. Eighty-three percent of those receiving unsolicited e-mail said the same thing. Finally, 81percent (unsolicited) and 88 percent (permission-based) of the consumers surveyed are likely to recommend the retailer to others. These are very powerful numbers that show that consumers do not view permission-based and unsolicited e-mail from retailers in a negative light. In fact, it is quite the contrary.

Registry Models Proposed by the Commission

NRF would like to address the feasibility of the e-mail suppression list models that were proposed by the Commission in its Request For Information ("RFI") issued on February 23, 2004.

Database of registered e-mail addresses

NRF has several key concerns about the creation of a database of registered e-mail users. First, we have concerns about the security of such a list. No such compendium of names, addresses, and e-mails currently exists, and it will prove to be very valuable to bad actors looking for live addresses to which to send spam. Currently, spammers have to do a great deal of guessing when compiling their e-mail lists including mixing thousands of common names and domains in the hopes of hitting upon a valid e-mail address. With this in mind, it will be important for the FTC to consider who will control the list. Will the FTC hold the list or will companies be allowed to download it to scrub against it?

Next, NRF strongly believes that any proposal for a national marketing e-mail suppression list must include a strong Existing Business Relationship ("EBR") exception and allow for consumers to give subsequent consent to receive e-mails from the individual businesses of their choosing. Such an EBR would be an adjunct to the transactional and relationship messages already exempted in the CAN-SPAM Act. In formulating this exception, the Commission will have to consider what constitutes both an EBR and subsequent consent. Will a convenient and customer-friendly checked box on a web site suffice? Or will the Commission require a more formal registration process with the retailer such as filling out and submitting a longer form with disclaimers? Also, will the Commission entertain some type of time limit on an EBR, as in the do not call rule?

Additional areas of concern to the retail industry are the extension of an EBR to individual salespeople or personal shoppers employed by a retailer, and an exemption for forward-a-friend programs. Often, salespeople keep in touch with customers who have specifically provided them with contact information and regularly update them on sales, purchases and the availability of merchandise via e-mail. Further, forward-a-friend programs are purely voluntary and highly successful programs that generate e-mails sent from the individual's e-mail address. The companies that use this type of tool offer it as a courtesy to their customers and generally do not capture or collect the e-mail addresses for future solicitations.

Finally, we are very concerned about the practicality and logistics of scrubbing against a national list that could potentially contain upwards of sixty million names (based on the current statistics compiled on the National Do Not Call Registry). How

will scrubbing work if one wishes just part of the list? Many retailers tailor their marketing to local or regional audiences -- how will list scrubbing work in these instances? Will the list be broken down by area code or zip like the do not call registry?

Other serious concerns remain as well. How much will compliance cost for businesses? How will small businesses with limited technology resources be expected to comply? Will constant list scrubbing get in the way of time-sensitive marketing such as holiday promotions, limited time offers, or price wars? Finally, what will the expected turnaround time be for the suppression of millions of names? Will marketers get more than just the ten days allowed for processing opt-outs under the CAN-SPAM Act? And finally, how will the Commission keep track of constantly changing and outdated e-mail addresses?

Domain-wide registry

The NRF is very concerned by the proposal included in the FTC's recent RFI that could create a domain-wide suppression registry. Under this model the ISPs and domain owners could totally control access to a retailer's customers whether or not a consumer chooses to receive e-mails from that retailer or make purchases on-line. Such a model could force retailers to pay a premium for advertising placement with ISPs, creating a huge competitive advantage for them in the advertising marketplace.

ISPs already have specific enforcement rights under the CAN-SPAM Act for individuals who engage in a pattern and practice of violating the requirements of the law. Giving the ISPs the ability to block domain-wide will only serve as a means to assign liability to businesses that are otherwise complying with their responsibilities under the

Act. To limit potential liability and uncertainty for senders, the FTC should consider, as with the database of registered users, how an individual using an e-mail address at a blocked domain will be able to opt back in with their favorite businesses and marketers. If the Commission adopts this model, clear attention will also have to be paid to how transactional, relationship, and EBR messages will be exempted.

Database of registered e-mail marketers

A database of registered e-mail marketers is not a new concept for many e-mail marketers. Many have been studying the idea of creating a "seal of approval" mark for legitimate commercial e-mail for sometime. (For example, The Network Advertising Initiative circulated a model entitled "Project Lumos" on August 15, 2003.) Under the model proposed by the Commission, best practice marketers would be issued a unique mark to embed in the body of their e-mail messages that would identify them as legitimate mail.

Several issues come to the forefront when considering this type of model. The first is what entity will decide who is an eligible marketer and what will the applicable standards be? One of the reasons the policy makers on Capitol Hill moved away from defining the term "spam" in the CAN-SPAM Act was because no one could agree on what exactly spam is. The term means many different things to different people, from pornographic and fraudulent mail to encompassing all commercial e-mail. Would the Commission run into the same problem in an attempt to set the parameters for approved e-mail marketers? It will not be easy to draw clear distinctions between good and bad e-mail.

Such a mark should also not be used to facilitate further blocking of commercial e-mail by the ISPs. In fact, if the Commission were to select this type of model, it would be essential to require ISPs to carry the e-mails of registered marketers.

Finally, the embedded marks issued by the Commission would need to be very secure. Clearly, the formula for these marks would become very valuable to bad actors eager to have their mail delivered to consumers' in-boxes. It would be imperative for the Commission to protect these marks from spoofing or hacking.

E-mail address and marketer registries with third party forwarding service

As the Commission is aware, marketers often use third party E-mail Service Providers ("ESPs") for the delivery of e-mail to their customers, and for market research related to these marketing campaigns. They are a valuable tool and provide valuable services. In investigating the feasibility of using designated e-mail forwarding services, the Commission would have to take into account several factors, not the least of which is will such a model put many valued ESPs out of business?

The Commission would have to consider the number of third parties approved for forwarding. Clearly the Commission would not want to approve too few ESPs – such a decision would inevitably create a bottleneck for commercial e-mail that could slow down delivery, especially at critical times such as the holidays or for time-sensitive sales and promotions. Furthermore, the Commission would not want to create any type of competitive advantage for one ESP over others, especially in the areas of delivery and market analysis. Finally, what standards will the Commission adopt to decide who may and may not be approved to provide this service?

Cost and security concerns should also be weighed by the Commission in determining the viability of this type of a model. How much would approved ESPs be allowed to charge for this service? Clearly, this model could create an environment ripe for price fixing or gouging. Security concerns not only cover the integrity of the e-mail addresses registered with the national e-mail suppression list, but also the security or confidentiality of the individual marketers' customer lists and marketing materials. If the only way a marketer can reach its customers is through an approved ESP, the Commission will need to take special care to define the parameters of the relationship.

A Do Not Spam Registry Will Not Be an Efficient Solution To The Spam Problem

Due to the many issues raised above, NRF believes that implementation of a Do Not E-mail Registry will not be a practical solution to the spam problem. NRF also believes that the creation of a Do Not E-mail Registry may create unrealistic consumer expectations. There will always remain a significant portion of the e-mail marketing community that will continue to flout the CAN-SPAM Act. These bad actors will likely also ignore the parameters of any suppression list and continue to fill in-boxes with spam. Further, spammers can easily move their operations offshore to avoid the jurisdiction of the Commission.

Just like the debate in Congress over the definition of "spam," different consumers may have different expectations over what type and volume of commercial mail could and should be blocked. A national Do Not E-mail Registry could potentially block *all* commercial e-mail, not just that mail that the average consumer characterizes as

spam. Consumers may be further puzzled by the many exceptions that would be needed to make the suppression list workable.

NRF and its members recognize the need to stop false and misleading e-mail and the proliferation of spam that is flooding in-boxes and jamming servers. A recent study published by the FTC showed that 66 percent of all e-mails analyzed by the Commission contained false or fraudulent "from" lines, "subject" lines or message text.[7] This is clearly unacceptable, however many of these abuses are now prohibited under the CAN-SPAM Act.

In the effort to further cut down on unsolicited e-mail, Congress and the Commission should keep in mind the effects that a Do Not E-mail Registry may have on legitimate marketers and their ability to communicate with their customers. Particularly worrisome is any suppression model that does not make clear exceptions for certain types of e-mail or does not allow for a consumer to consensually receive e-mail from a marketer. Without such protections the registry may only act as an incentive for litigation and enforcement actions against legitimate businesses that are otherwise complying with the requirements of the Act.

The Internet has provided many Americans with unprecedented access to consumer products, particularly for consumers in underserved or rural areas. However, in order to communicate with our customers in this medium, retailers must use e-mail. As more and more spammers move offshore to evade the long arm of the law, will it be the retailers and legitimate marketers who ultimately pay the price for the spammer's misdeeds? Clearly, we hope not.

---

[7] "False Claims in Spam," a report by the FTC's Division of Marketing Practices, April 30, 2003.