THE NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

March 29, 2004

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary
Room 159-H
600 Pennsylvania Ave., N.W.
Washington, DC 20580

Re: CAN-SPAM Act Rulemaking, Project No. 41108 - FTC Study on Do Not E-Mail Registry

Dear Mr. Secretary:

On behalf of the National Business Coalition on E-Commerce and Privacy, we are pleased to have the opportunity to submit comments on the FTC's study for a proposed Do Not E-mail registry.

The National Business Coalition on E-Commerce and Privacy is comprised of nationally recognized companies from diverse economic sectors dedicated to the pursuit of a balanced and uniform national policy pertaining to electronic commerce and privacy. Our member companies are top competitors in the e-commerce marketplace, and are strongly committed to ensuring the privacy and security of our customers, both on-line and off-line.

As some of America's most reputable companies, we know that it is in our interest to market only to those customers who wish to hear from us. We are deeply concerned about the problem of false or misleading e-mail advertisements. The credibility of legitimate companies who market and advertise through electronic mail is damaged when e-mail is perceived as being either deceptive or a nuisance.

While we were pleased by the recent passage of the CAN-SPAM Act, we do not believe that a Do Not E-mail registry will help solve the spam problem – and it could make the problem of false or misleading e-mail even worse. Quite simply, we do not believe that there is any way that such a registry can be made to serve its intended purpose and it could even pose new threats to online security. The technical, privacy, and security difficulties of creating a Do Not E-mail registry will likely pose insurmountable obstacles.

JOHN SCHALL
EXECUTIVE DIRECTOR

601 PENNSYLVANIA AVENUE, N.W.
NORTH BUILDING, 10TH FLOOR
WASHINGTON, DC 20004-2601 USA
202.756.3385
FAX - 202.756.3333
JSCHALL@ALSTON.COM

The fundamental problem is that any public registry could be accessed and abused by bad actors. Those businesses that are operating legitimately would, of course, abide by their customers' decisions not to receive advertising via e-mail. The problem, however, arises with the illegal spammers and hackers – those who will send out 14 billion unwanted or fraudulent e-mails this year alone. For such lawbreakers an e-mail registry could serve as an easily accessible and exploitable address list. Paradoxically, then, a registry would benefit spammers while doing little or nothing to enhance information security or reduce unwanted e-mails

Equally important, the problem of spam is not the same as unwanted telemarketing. Nor is it the case that a Do Not E-Mail registry for spam would be analogous to a Do Not Call list for telemarketing. The technologies of e-mail and telemarketing differ significantly. Unlike telemarketing, which is easily traceable, current unsecured Simple Mail Transfer (SMTP) e-mail technology makes it possible for spammers to falsify or obscure sender information. This is further complicated by the fact that much spam originates from overseas and is beyond the reach of American law enforcement.

There have been several proposed alternative approaches to a registry including: a simple list of e-mail addresses; the creation of a domain opt-out; a Do Not E-mail list held by a third party; and a registry of authorized marketers. Generally, these systems suffer the same practical defect: the technology of concealment is almost foolproof, making enforcement of the Do Not E-mail registry extremely problematic. Further, some of the proposed approaches, such as the domain opt-out, would have the potential effect of blocking all e-mails going to a specific domain – even if they are legitimate. Moreover, any e-mail registry combined with anti-spam filters already in use by ISPs could prevent legitimate messages from lawful senders from getting through.

We do believe that a competitive marketplace will yield technical solutions, and we are strongly supportive of emerging technologies. We are hopeful that still emerging technologies like the "verified sender model" will prove more effective than the Do Not E-mail registry and may contribute to solving the spam problem. Such an approach can create transparency among senders of volume e-mail so that any consumer could confidently decide what e-mail they want to receive and which they do not. The "verified sender model" eliminates spam by holding all volume senders accountable for the e-mail they send and for their sending practices.

Given the real world technological and enforcement difficulties, we do not believe that there can be an effective Do Not E-mail registry that would be both secure and enforceable. Notwithstanding all of the practical difficulties associated with a registry, however, we understand and appreciate that the FTC is required by the CAN-SPAM Act to write a report setting forth a plan for a Do Not E-mail registry. We strongly believe that the FTC's report setting forth a plan should include the following elements:

- *Uniformity and Preemption.* Nothing is more interstate in nature than the Internet. To avoid exacerbating the already complicated compliance environment created by conflicting state laws, any plan for a Do Not E-mail registry must provide for uniformity across the nation and the preemption of state and local laws – just as the CAN-SPAM Act itself is preemptive.

- *Preexisting Business Relationship Exemption.* Because consumers who place their e-mail address on a Do Not E-mail registry would still expect to hear from companies with whom they conduct business, any Do Not E-mail registry should provide an exemption that would allow businesses to send transactional, informational, and promotional e-mails to those with whom they have pre-existing relationships.

- *"Affirmative Consent" Exemption.* A Do Not E-mail registry must allow for an "affirmative consent" exemption that permits consumers to continue to receive information from those companies from whom they had previously agreed to receive information. Honoring such company specific consumer opt-ins would also be consistent with the intent of the CAN-SPAM Act as we understand it.

- *Business to Consumer Coverage.* Any Do Not E-Mail registry should apply to business-to-consumer relationships only, and not to business-to-business relationships. At a minimum, in business-to-business relationships, only the company that owns the asset of an e-mail address should be able to block e-mail to it, thereby allowing businesses to set a single corporate wide e-mail policy.

If you have any questions or would like a further elaboration of our views, feel free to call me at (202) 756-3385. We look forward to continuing to work with you as you seek to develop the regulatory structure pursuant to the CAN-SPAM Act.

Sincerely,

John A. Schall
Executive Director