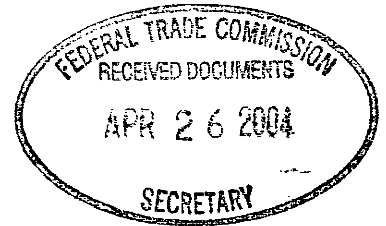
001156



BAKER
&
HOSTETLER LLP
COUNSELLORS AT LAW

WASHINGTON SQUARE, SUITE 1100 • 1050 CONNECTICUT AVENUE, N.W. • WASHINGTON, D.C. 20036-5304 • (202) 861-1500
FAX (202) 861-1783

April 20, 2004

Via Elecronic Mail
and First Class Mail

Donald S. Clark, Secretary
Office of the Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: CAN-SPAM Act Rulemaking, Project No. R411008

Dear Mr. Secretary:

Baker & Hostetler LLP is pleased to submit these comments to the Federal Trade Commission ("FTC") concerning the CAN-SPAM Act rulemaking proceedings. Baker & Hostetler LLP is a national, full-service law firm representing clients from all types of industries ranging from major publishing, high tech entities to small entrepreneurs and direct marketers. The sending of commercial e-mail and the regulations promulgated under the CAN-SPAM Act affects our clients from all industries.

Our clients agree with and support the goals and the intent of the CAN-SPAM Act. However, some of the provisions under the Act are ambiguous and have created confusion, which has interfered with legitimate online advertising programs that have served consumers' interests in receiving relevant, compelling commercial e-mail. We wish to explain one of the main issues that have frustrated legitimate business efforts, particularly in the management of highly proprietary customer lists.

The definitions of "sender" and "initiate" are ambiguous and appear to be at odds with the long-standing practices of businesses engaged in direct marketing. For the reasons set out below, the definitions could force businesses to divulge customer names that they would ordinarily work to protect and often have promised to protect. Ironically, from a consumer standpoint, the current definitions could weaken privacy practices and expose consumers to more, rather than less, unsolicited commercial e-mail from unscrupulous advertisers.

Under Section 3(16) of the CAN-SPAM Act, "sender" is defined as "a person who initiates [a commercial e-mail message] and whose product, service, or Internet Website is advertised or promoted by the message." "Initiate" means "to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message." Section 3(9) of the CAN-SPAM Act. The definition of "initiate" specifically states that more than one person can be deemed to "initiate" a commercial electronic mail message. It is also clear that more than one person can be deemed the "sender" in some circumstances.

The "sender" of the commercial e-mail is required to comply with the opt-out provisions and other provisions of the Act. Under Section 5(a)(3) of the CAN-SPAM Act, it is unlawful for a person to "initiate" a commercial e-mail without a mechanism by which the recipient may opt out of receiving future commercial e-mails. It also is unlawful for a person to initiate a commercial e-mail message without disclosing clearly and conspicuously the existence of such mechanism and a valid physical address of the "sender." Section 5(a)(5) of the CAN-SPAM Act.

Complying with the CAN-SPAM Act requirements is clear for advertisers who compose commercial e-mail and send it from their own domain(s) using the advertiser's own e-mail list. But, realistically, those types of situations are in the minority for most major advertisers. Our concerns arise when the entity whose product or service is advertised is *not* the same entity who owns and controls the lists of consumers and sends the advertiser's message for a fee or otherwise.

Commercial e-mail is simply another form of advertising. Like non-electronic marketing methods, creating, maintaining and selling names and addresses of targeted consumers is a very useful and, sometimes, independent business. Working with list owners is cost effective and avoids disturbing consumers who are unlikely to respond to the advertisements. It provides an inexpensive method for businesses to locate and reach interested customers.

As with traditional postal address lists, e-mail lists are extremely valuable and normally are closely held as proprietary information, whether by the advertiser or the list owner. Advertisers often create their own lists through various means. For example, they may obtain prospects through their own websites, in which interested consumers actually agree to receive future solicitations and offers from the advertisers. They may also amass e-mail addresses of prospective customers through offline and online direct response marketing efforts. Prior to the CAN-SPAM Act, legitimate e-mail advertisers recognized the privacy concerns of their customers and honored voluntarily any requests *they* had received to discontinue future e-mailings.

Problems arise under the CAN-SPAM Act, however, when advertisers contract out for the services of third parties using the third parties' own e-mail lists and send the advertiser's message to their own list. These third parties obtain and maintain their lists in similar ways as the advertisers. They often maintain not only one list, but also may have many lists each targeted at a specific demographic, product mix or consumer choice. For clarity, typically in the

industry, these list owners provide an opportunity for customers to sign up to receive information from the list owner and their partners about products and services. This information is gathered in the context of a relationship between the list owner and the customer in which the customer is also signing up for and/or buying products and services from the list owner. These list owners then follow up with commercial e-mail that identifies the third-party list owner as the "sender," reminds the consumers that they previously agreed to receive such mailings, and provides an opt-out mechanism. Under this scenario, the consumers' expectations are that the e-mails originate from the list owner and that, if they choose to opt-out of future e-mailings, the opt-out will apply to the future e-mails of only the third-party list owner. We doubt that reasonable consumers under this typical scenario would anticipate that such an opt-out would apply to all e-mailings regarding the specific third-party advertised product, and all that implies.

Maintaining the confidentiality of, and control over, these lists by the list owner, whether that owner is the advertiser or the third-party list owner, is of utmost importance. Advertisers who contract with third parties to solicit potential customers on their behalf typically do not share, and do not want to share, with those third parties their own proprietary e-mail lists. Similarly, the third parties who offer e-mailing services do not want to share their proprietary lists with multiple advertisers. Rather, all list owners want to control e-mail list information and the customer experience, as they would all customer lists, and other sensitive business information, electronic or not.

Prior to the enactment of the CAN-SPAM Act, the industry standard was that the entity that controls the e-mail information honored the opt-out requests of recipients. All communication from the consumer was with the entity that controlled the e-mail address and mailed the solicitation. In fact, in situations where the e-mail address is generated from opt-in requests from potential customers, the potential customer reasonably expects that future communication will be between the customer and the entity that sought the customer's permission to send e-mails.

However, the CAN-SPAM Act does not reflect these realties of common e-mail sending practices. Defining the "sender" to a way that could include both the advertiser and the third-party list owner, regardless of which entity actually controls the e-mail address list, creates anomalies, some of which actually go against the purpose of the CAN-SPAM Act and against consumers' interests as well. Confusion lies in determining which entity must honor the recipient's opt-out request and from which of their lists. It is not clear if an unsubscribe request must be honored both by the advertiser (or in some cases multiple advertisers) and by the third-party list owner, or if the request pertains only to the list owner who controls the database and uses its own domains to e-mail the message. If the FTC defines "sender" to include both the third-party list owner who obtained the recipient's agreement for future e-mail solicitation and the advertiser(s), a logistical nightmare results.

For instance, an advertiser who maintains its own e-mail data bases may engage in an e-mail campaign that involves both e-mails sent from the advertiser's domain and from the domains of multiple third-party list owners. They all are sending the same advertisement, the

contents of which originates from the advertiser. Each of the four third-party list owners has four different databases. One of the third-party list owners receives 2000 opt-out requests from its e-mail solicitation. Does the CAN-SPAM Act require that third party to share those 2000 names (which originate from its own proprietary databases) with the advertiser or multiple advertisers using their services? Must those advertisers then add those e-mail addresses to their respective data bases for suppression purposes? Are those advertisers then required to share with the other third-party list owners, whom they will use for future solicitations, the e-mail addresses on the suppression list?

If this "sharing" of information is required by the Act, the burdens and financial and other costs imposed are so significant that legitimate e-mail campaigns will be thwarted. List owners and advertisers alike would have to devote tremendous time, money, and effort to create and use such sharing mechanisms. Such mechanisms do not exist today and are technically very difficult to create and implement. The result simply is that few could meet the requirement that opt-out requests be implemented within 10 days of receipt.

Beyond that, the "sharing" will have a chilling effect on legitimate advertising. The original third-party list owner will be less willing to accept advertising to its proprietary names. Moreover, list owners will simply refuse to share their lists, especially if it means its competitors could thereby receive access to them. It is an untenable situation that does not reflect sensitivity to the proprietary and competitive nature of the database holders.

In addition, such "sharing" often goes against list owners' privacy policies that state that any personal information collected will *not* be shared. Consumers who rely on such privacy policies have a reasonable expectation that by giving the website their personal information it will not be used to increase the amount of unsolicited commercial e-mails they receive. Yet, as explained more fully below, the consumer's information might have to be shared with many entities.

The net result is that third-party list owners (and advertisers) do not wish to open up this series of potential privacy violations for their customers or incur the expense of creating a system to deal with the opt-out requests. Instead, some have eliminated this option altogether as an advertising channel, significantly limiting or reducing cost-efficient advertising opportunities for legitimate businesses, and reducing advertising revenues for list owners.

More alarming, this situation also can harm consumers. The e-mail addresses of the 2000 recipients who wished to opt-out would be shared with at least five entities under this hypothetical scenario, thereby risking the likelihood that those e-mail addresses will find their way to additional data bases from which other advertisers' commercial messages will be sent. Worse yet, the scenario creates enormous potential for the stealing or hijacking of e-mail addresses. Stealing or hijacking can occur as a result of either an intruder who hacks into one of these five computer systems or an illegitimate company that masquerades as a legitimate list owner who provides e-mailing services to third-party advertisers. Third-party advertisers unknowingly may share the suppression list with this masquerader who then shares or sells its

services to unscrupulous serial spammers. And, some opportunistic advertisers or third-party list owners will use the distributed names to build other data bases, the opposite of the consumer's request. In general, the broader the distribution of the list owner's suppression files, the greater the likelihood that consumers' e-mail addresses will land in the hands of an unscrupulous hijacker, hacker or masquerader who can then use the suppression list for fraudulent or pornographic unsolicited commercial e-mails.

Consumers also are likely to be confused and may not succeed in effectuating their opt-out requests. In existing relationships, consumers have opted into list owner's requests to receive future e-mail offers and promotions from the list owner and other advertisers who are selected by the list owner. Consumers opt into these services precisely because they know that the list owner will adhere to its privacy policies, which typically state the list owner will keep the e-mail addresses confidential by not sharing them with advertisers and will honor all future opt-out requests at any time. Usually, the future promotional e-mails are identified as originating from the list owner as the consumer expects, and third-party advertisements are obvious and usually marked as such. Here is an example of such a disclosure and it was placed at the very beginning in the body of the commercial e-mail. "The following is a special offer for [list owner] subscribers from our sponsor, [name of advertiser.]"

Consumers know that their relationship is with the list owner. Those who exercise their opt-out rights will expect that the list owner with whom they have the relationship, not the third-party advertiser, will operate the opt-out mechanism and suppress their names from future e-mails from that list owner. If the definitions do not reflect both sound business practices and the consumer's understanding and expectation, the consumer may be left confused or frustrated by what their opt-out request actually yields. Unknowingly, the consumer could be providing their e-mail address to the advertisers with no real knowledge of how that address will be transferred and communicated and in the process may not even succeed in removing themselves from the list they were on in the first place.

Frankly, consumers who are bombarded with spam from unscrupulous spammers are hesitant to effectuate opt-out requests if they believe that their e-mail address will be given to persons outside a relationship in which they have previously given consent. Indeed, before the CAN-SPAM Act, consumer groups advised consumers NOT to reply "unsubscribe" because of the fear that it would confirm a "live" e-mail address.

Since passage of the CAN-SPAM Act, some list owners, who are concerned about how to comply with the Act while still maintaining advertising revenues and database size, have resorted to including language in third-party advertisements informing customers that by exercising their opt-out requests, their names will be forwarded to third-party advertisers and that the list owner is not liable for the actions of those third-party advertisers. This is an example of such a notice being used currently.

> "You are receiving this email from [list owner] because you chose
> to receive messages from [list owner's] partners on the [list

> owner's] web site(s). Please note that [list owner] does not produce or endorse this product, and assumes no responsibility for the use thereof. You understand that by opting out you are transferring or authorizing the transfer of your email address to the advertiser listed below. [List owner] has no control over how your email address is used by the advertiser or other third parties. Accordingly, [list owner] disclaims all responsibility and liability arising from the subsequent use of your email address that is made possible by your submission of your email address below."

Our clients believe this type of notice has diminished the exercise of opt-out rights because consumers fear that their names will be forwarded to an advertiser or other unknown parties with whom they have no contact, rather than the list owner with whom they have a relationship, and placed advertisers in an unworkable arrangement.

The solution is to give both control *and* responsibility to the entity that owns or controls the list of e-mail addresses and has the relationship with the consumer. The FTC should define "sender" (and "initiate," if necessary) to mean "that entity who controls, maintains or owns the database" and with whom the recipient presumably has a relationship. Alternatively, the FTC can narrow the definition of "sender" by creating an exception that would exclude those third-party advertisers who do not own or control the list or where the list owner does not transfer e-mail addresses to the third-party advertisers. Under such a definition, more than one party could be the "sender" of an e-mail, if the e-mail address list is owned by two or more entities.

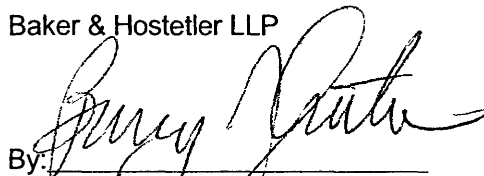
By defining "sender" in this manner, the FTC will place the responsibility of ethical data base management on the parties who actually gather names into a data base, while minimizing privacy concerns for consumers. It would require that any entity that collects e-mail addresses with the intention of distributing advertising to maintain a reasonable method for tracking the opt-out requests from consumers. It also motivates the third-party list owners to self-police the advertisers for whom they do business. Those third-party list owners will want to screen their advertisers to avoid significant levels of opt-out requests, which, in turn, would directly impact on the size of the list owner's data bases and the list owner's ability to generate profits.

In sum, defining "sender" in this manner will improve the ability of the Commission to enforce the requirements of the Act and will mirror the current standard within the advertising industry. In addition, the FTC's action will reflect reasonable consumer expectations in that the entity with whom the consumer has a relationship will effectuate their opt-out requests and will not share their personal information with others. It will decrease the potential of unscrupulous spammers, hackers, and hijackers from gaining access to the suppression lists. Finally, third-party list owners who have existing relationships with the consumers will be motivated to ensure that their advertisers' and their own promotions are legitimate and unlikely to provoke high numbers of opt-out requests.

We thank the FTC for considering our comment and appreciate the opportunity to submit our views.

Sincerely,

Baker & Hostetler LLP



By: ______________________

Barry J. Cutler
Julia A. Oas