March 31, 2004

Federal Trade Commission
Office of the Secretary
Room 159-H
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: CAN–SPAM Act Rulemaking, Project No. R411008
National Do Not E-mail Registry
RIN 3084-AA96

Gentlemen:

MBNA America Bank, N.A. ("MBNA") is pleased to respond to the Advance Notice of Proposed Rulemaking issued by the Federal Trade Commission ("FTC" or "Commission") (69 Fed.Reg. 11776, (2004)). Specifically, MBNA's comments relate to the report required under Section 9(a) of the CAN-SPAM Act (the "Act") mandating the Commission to set forth "a plan and timetable for establishing a nationwide marketing Do Not E-mail Registry."

We welcome the passage of the CAN SPAM act as a first step toward attacking the problem of spam. As a reputable company and legitimate marketer, we believe that it is in the best interest of all to market only to those customers or members 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 that market goods and services through e-mail is being damaged by the conduct of spammers.

Overview

While we agree that further efforts are needed to address the spam problem, we do not believe a national registry is the appropriate solution. There are two fundamental problems with such a registry:

- First, the practical realities are that any such registry would have to be widely and easily accessible to marketers, ISPs, domain owners, and others, which also makes it easily accessible to spammers;
- Second, the open architecture of the Internet facilitates spamming because of the lack of geographical boundaries and effective security mechanisms, which makes it difficult to identify spammers.

Implementation of such a registry simply will not work in this setting. Spammers will seize the opportunity presented by such a registry to propagate its e-mail addresses worldwide.

Additionally, U.S. consumers will ultimately bear the tremendous costs associated with use and maintenance of such a registry, while being exposed to its risks.

In addition to security concerns, a national registry presents several operational problems. Transmitting the registry database would be unwieldy for smaller and less technology-sophisticated businesses. The necessary suppression steps would make it extremely difficult to meet the ten-business-day opt-out requirements and would severely limit a marketer's ability to deliver its products and services.

While we believe the problem must be addressed, we believe that any proposed solution must address the real problem and must recognize the practical realities of the Internet. The real problem is the inability to identify accurately the e-mail sender. Spammers on the Internet are able to conceal their identities. For this reason, we support private industry's efforts to develop a "verified sender model." While we may be a few years away from the ultimate model, we believe this is where the FTC should focus its efforts. Any plan should focus on evaluating, in coordination with industry, practical solutions to this worldwide problem. Additional legislation that burdens legitimate marketers is not the answer.

However, if the Commission chooses to implement some form of registry, the Commission should at a minimum provide an established business relationship exemption for marketers so they can service their existing customers' needs. Also, the ten-business-day rule should be extended to at least 30 days.

In an effort to provide you with further information regarding the creation of a national registry, the following comments detail our responses to the questions in the ANPR.

1. ***What practical, technical, security, privacy, enforceability, and other concerns exist with respect to establishment of such a registry?***

   We assume that one of the models contemplated in the Request for Information ("RFI") would be at the core of any solution that might be adopted. There are two basic types of registry being proposed:

   (a) a do not e-mail registry comparable to the national do not call list; and
   (b) a registry of do not e-mail domains.

   The main questions are:
   - What type of registry should be adopted?
   - How will the registry be accessed?

National Do Not E-mail Address Registry

- **Security**

The primary weakness of this model is security. Regardless of the access method established, a central database having an estimated 300,000,000 e-mail addresses presents the ultimate target for spammers, hackers, etc.

The open architecture of the current Internet e-mail system presents a structural risk. When an e-mail server receives a message, there is no sender authentication, i.e., it is delivered to the recipient "as-is" with no way to verify the identity of the sender or the originating domain. Given this architecture, an unscrupulous competitor could easily sabotage a company by sending undesirable e-mail messages to a company's customers using the source address of the victimized company. For this and other reasons, we must develop and adopt a security mechanism for the reliable identification of senders.

- **Digital Certificates**

While some security mechanisms are in place to secure the central registry, their deployment is limited and the feasibility of their use on a worldwide basis is doubtful. Digital certificate technology has proven to be effective. A digital certificate is an electronic affidavit issued by a certification authority that validates the identity of an individual or business sender. Unfortunately, the costs associated with the deployment of a digital certificate regime and the requirement for significant investment in a central user repository make it an expensive alternative. Additionally, a mechanism requiring digital certificates would involve the establishment of a global "trusted third party" that would issue the certificates and be accepted by all systems.

Secure identification mechanisms such as digital certificates would require the development of security standards in every e-mail client. Further, it could not be enforced until the natural attrition of e-mail clients that do not meet the standards is completed (approximately 7-10 years). Internet encryption companies experienced a similar problem in offering digital certificates for secure web transactions. A move to a stronger encryption standard required all Internet users to upgrade to a fairly recent version of web browser. Many Unix browsers, for example, are still not compliant and will not allow users to access high-security web sites. If the same approach were applied to e-mail, it would cause similar costs, complications, and difficulties.

- **Hashing**

One method for deploying a "do-not-email" list that shows promise is the use of "one-way hashing." This method would involve processing each e-mail address using an encryption algorithm that creates a string of characters ("hash") representing the e-mail address. Each hash would be unique and could not be reverse-engineered to the original address. Marketers could compare the hashed versions of their e-mail list to the hashed versions of the "do-not-email" list and remove any matches. This would ensure e-mail addresses were not

compromised or gleaned from the list. Unfortunately, this would not circumvent the primary problem associated with offshore or dishonest marketers, who would disregard the list and continue sending spam as they currently do.

- **Free E-Mail Accounts**

All existing "free" e-mail accounts (Hotmail, Yahoo, etc) would have to be deleted and those offerings removed. These systems allow zero-authentication accounts to be created for very short periods of time. Since identities of their users are never confirmed, spam could be sent from hundreds of these addresses with no way to track it back to the offender.

- **Verification of Identity**

Even if the technical problems associated with wide-scale use of sophisticated security mechanisms could be addressed successfully, there would be other avenues available to spammers. For example, how does one ensure the legitimacy of every entity that registers as a legitimate user? A simple example would be where a "charity" that is a front for some other organization (e.g., terrorist) disguises itself as a legitimate operation to fraudulently obtain e-mail addresses from the registry and spam consumers. They could also compound the problem by "phishing" for confidential information from the consumers with the compromised e-mail addresses.

We believe further study should be undertaken concerning the feasibility of a secure, unique identifier for each entity engaged in e-commerce. Several industry groups (such as Tumbleweed Communication's Working Group) are currently studying the problem of mutual authentication in e-mail environments. Mutual authentication is a mechanism employed by two parties for the purpose of proving each other's identity to the other before e-mail communications are transmitted.

Although no feasible solution currently exists, there is widespread opinion that any solution must be (a) accepted globally by all software developers and consumers, and (b) provide a true authentication of the origination of the message by using validation techniques including certificates, biometrics, credit card, etc. to prove identity.

- **Operational Problems**

There are many operational and practical problems, the most significant of which is the large number of e-mail accounts to be evaluated. In the event that all marketers' lists had to be compared to a centralized list, a critical bottleneck would occur. Specifically, having approximately 500,000 marketers comparing their lists to an estimated 300,000,000 e-mail addresses at any one time would not be feasible. This would cause excessive turnaround times for marketers to have their e-mails distributed.

- **Periodic Validation**

In order to maintain the accuracy of the register, all ISP's would have to review the database periodically to ensure the continuing validity of all addresses in their domains and have the ability to update addresses. Costs for providing e-mail service to customers would likely soar for both the customers and the ISPs. The access models in the RFI imply that the database would be distributed (potentially monthly) in some fashion, a process that would raise security concerns as previously mentioned. Also, it would be a crushing burden if companies were required to download the database every day to keep it up-to-date.

- **Adverse Impact on Small Marketers**

Another practical implication of a single central registry that requires sophisticated security and transmission features is that many small, legitimate marketers would simply not have the technical capabilities to access the registry and would be forced to cease using e-mail as a marketing channel. The result would be competitive inequity between large and smaller marketers.

- **Privacy**

Many consumers have multiple e-mail accounts, e. g., one address for family and friends, and another address for open use on the Internet. The consumer would likely want the private address protected from spam and from unwanted marketing. If the registry were to be compromised or accessed by spammers or other unscrupulous users, these private e-mail addresses would become public.

The registry database would have to be transmitted to those companies that market via e-mail. Due to the questionable practices of some companies, there is little chance that addresses on this registry would remain confidential. The database only has to be compromised once for its value to be degraded and e-mail addresses transmitted throughout the Internet.

- **Enforceability**

Enforceability presents unique challenges. If a spammer breaks into or compromises the registry, it would be difficult to determine which security mechanisms of the ISP, marketer, or FTC were breached. The problem of controlling information and security in the registry should not be viewed in isolation from the Internet and its complex network of users, providers, and infrastructure.

The U.S. cannot enforce its anti-spam laws in other countries where a high percentage of spam originates. And U.S. companies that want to circumvent the registry would only have to set up a re-mailer system in a foreign country that would deliver messages to U.S. consumers from a foreign address.

- **High Maintenance Cost**

Maintaining a national registry would be extremely expensive. It would require access administration, file management, monitoring, and other routine operational processes, together with qualified support staff.

- **Conclusion**

For all of these reasons, we do not believe a national do not e-mail registry would be a realistic or cost-effective solution to the spam problem.

National Do Not E-mail Domain Level Registry

A domain level registry would consist of solely of domain names registered to avoid receiving unwanted e-mail. For example, all of Yahoo could be a domain. If Yahoo sent in its domain name to the central registry, none of the e-mail addresses attached to that domain would be eligible to receive e-mail. None of the e-mail addresses would be housed in the central registry - only the Yahoo domain name. Thus, a spammer would be unable to obtain an individual e-mail address related to the domain name by obtaining the Yahoo domain name from the central registry. The advantages of a domain level registry would be that e-mail addresses would not be resident in one place and thus open to compromise.

However, the model would likely spawn a host of domain level entities set up to collect do not e-mail addresses to be fed to the central registry. Some of these would be legitimate; some would not. The unintended result would be distributed databases of e-mail addresses, possibly administered by the wrong people. Regardless of whether the domain owner was good or bad, the same security issues would be involved as in the centralized model.

The bigger concern with this model is that it shifts the registration choice from the recipient to the domain owner. With this model, any of the approximately 30,000,000 domain names (RFI assumption) could register. What would happen to recipients who want to receive e-mail from certain businesses, but are attached to domains that register with the registry? The net result of this model would be to disenfranchise recipients who are loyal to certain companies and to impair significantly the effectiveness of the e-mail channel for legitimate marketers. Since e-mail addresses do not have the portability that cell phone numbers enjoy, a recipient who has committed to a specific e-mail address and has communicated it to his or her contacts, might find it impractical to change e-mail providers. If an individual recipient or business does not agree with the domain owner's choice to register, they might not have the option to replace that owner with another domain without significant inconvenience or disruption.

This model would also create a central bottleneck. If marketers access the registry, there could be as many as 500,000 marketers trying to access a list of up to 30,000,000 domain names.

- **Conclusion**

For all of these reasons, we do not believe a national do not e-mail registry would be a realistic or cost-effective solution to the spam problem.

Registry Access Methods

The RFI describes three models of access to a centralized registry: registered marketers, registered ISPs and domain owners, and registered third-party forwarding services.

- **Lack of Boundaries**

While each of these methods attempts to isolate access to the centralized registry in a controllable manner, none of them can overcome the issues caused by the Internet's open architecture. The methods assume that artificial country boundaries can be placed on the Internet and that effective e-mail security solutions can be instituted within the U.S. or abroad. These are not, and may never be, practical solutions. In fact, the open architecture of the Internet is inconsistent with these assumptions, as it was established to promote open exchange of electronic communication around the world. For any access method to work, existing e-mail protocols must be fundamentally changed.

- **Distribution, Transmission, and Suppression**

Additional operational concerns with each of the access methods make them problematic. Each method would require database distribution capability to avoid bottlenecks. As stated previously, any database distribution process would create increased security risk. Additionally, transmitting the database with any frequency would not be practical given its necessarily large size. Some access entities would not even be equipped to receive a registry of this size. The suppression files, which are necessary to meet the ten-business-day opt-out requirements, create technological challenges and severely limit marketers' ability to deliver their products and services.

- **Conclusion**

We believe that the best approach to the spamming problem is to ensure that senders of e-mail are legitimate. For this reason, we believe the FTC should follow the approach being taken by several business consortiums, which is to develop a "verified sender model." Of the methods proposed, the registered marketer regime appears the best approach to a solution of the sender identification problem. However, we believe it is premature for the FTC to attempt to define the components of an ultimate technical solution. Instead, we think the FTC should support industry experts who are already working on the problem. The ultimate solution may not entail any form of registry, but rather, a change in e-mail security protocols that would prevent the sender from hiding its identity. While there would still be offenders, their appetite for sending spam would decline significantly due to the ease with which they could be found and prosecuted.

Can these concerns be overcome so that a registry would be workable and effective?

We believe the technical challenges and risks inherent in either a central do not e-mail registry or a central domain registry cannot be overcome at this time. The security and operational challenges are simply too great to develop a commercially workable and reliable registry that would meet the demands of consumers and marketers.

If so, what might be an appropriate plan and timetable for establishing a registry?

Given the numerous fundamental problems with establishing a national registry, we do not believe a plan of implementation is practical at this time.

Is such a registry a practical, efficient, and workable method of solving the spam problem?

We do not believe this is the correct approach to eliminating spam.

What are the relative costs and benefits?

We do not believe that a centralized registry would provide any significant benefits to consumers or industry; in fact, they would be harmed by the risks we have discussed. We believe the only parties to benefit would be spammers. We believe that the cost would be enormous and would ultimately fall on the consumer, especially the U.S. consumer. Large marketers with technical capabilities to interface with such a registry would ultimately pass along their costs to consumers. Smaller marketers that are less sophisticated technically would be unable to justify using the e-mail channel, which would also impact consumers since they would have less choice available on the Internet.

2. ***How could such a registry be structured and applied to best protect children with e-mail accounts?***

Our concern with such a registry is even greater as it pertains to the protection of children. For the many reasons we have stated, children's e-mail accounts would be exposed to spammers if contained in such a registry. Because we feel strongly that such a registry would ultimately be compromised no matter how it is structured, we believe children's accounts should not be contained in such a registry.

Could such a registry be effective as a means to protect children from inappropriate spam?

We do not believe such a registry would protect children, but would in fact expose them to further unwanted access by purveyors of inappropriate content.

* * *

Thank you for your consideration in this matter. If you have any questions, please contact the undersigned.

Respectfully submitted,

MBNA America Bank, N.A.

by: /s/ Joseph R. Crouse
Joseph R. Crouse
Legislative Counsel
(302) 432-0716