

### **Additional Comments regarding the FTC Questionnaire:**

In modifying the Act's definition of "commercial electronic mail message," the term "the primary purpose" could be interpreted in many ways. Click the choice below that most closely matches your view of the correct interpretation.

2. Should the identity of an e-mail's sender affect whether or not the primary purpose of the sender's email is a commercial advertisement or promotion?

No

It is common practice to come up with catchy "handles" for an email sender identity. Also as the internet grows, choices for sending names become very limited. Finally, for companies who are marketing, they must exercise some protection for their workers who are harassed by crazy people and anti-spammers.

3. Are there other ways to determine whether a commercial advertisement or promotion in an email is the primary purpose of the email?

No

An email is of a commercial nature with its primary purpose as commercial when it is promoting a product or service to a consumer or a potential consumer. Americans are intelligent enough to see when a product or service is being advertised. It is not necessary to complicate this area.

### **B. Modifying what is a "transactional or relationship message".**

Under the Act, a "transactional or relationship message" is defined as meeting one of seven criteria. As indicated in the choices below, the criteria relate to, for example, whether the message: concerns prior or already-established commercial transactions between sender and recipient; products or services purchased by the recipient; or an ongoing commercial or employment relationship between sender and recipient.

1. Choose any of the definition(s) below that you feel the Commission should modify or elaborate upon. (Choose all that apply)

None of the above, the term "transactional or relationship message," as defined in the Act, is clear, and needs no further clarification or modification.

2. Have any changes in electronic mail technology or practices occurred since the CAN-SPAM Act became effective on January 1, 2004, that would necessitate modification of the Act's definition of "transactional or relationship message" to accomplish the purposes of the Act?

Yes

I know of two clients that are unable to send updates and notifications to users at many ISPs (who have requested information from them) due to new filtering techniques employed by the ISPs. Very often this is due to the fact that ISPs are filtering any email with a URL in it. Thus transactional or relationship messages are being eliminated from the net. My clients for example have had to resort to using the fax machine for many routine communications that we once sent by email due to the website being a part of that email message and thus not forwarded to the intended recipient by the ISP.

ISPs need to be instructed to back down their filters or reset their filters to allow federally compliant email, and transactional and relationship email as well. They have filters set so tightly that it is very difficult to send or receive from your personal email program.

3. Some transactional or relationship messages may also advertise or promote a commercial product or service. In such a case, is “the primary purpose” of the message relevant, and if so, what criteria should be applied to determine the “primary purpose” of such a message?

No, the primary purpose of the message is not relevant. By virtue of the concept of a transactional or relationship message, the government, and the ISPs should have no jurisdiction or say in what the two parties communicate. Once a relationship has been established it is no longer the concern of any regulatory agency or private company.

4. Should transactional or relationship messages that also advertise or promote a commercial product or service be deemed “commercial” messages or should they be deemed “transactional or relationship” messages?

They should be deemed “Transactional or Relationship” messages

### **C. Modifying the 10-business-day time period for processing opt-out requests.**

1. Is 10 business days an appropriate deadline for acting on an opt-out request by deleting the requester’s email address from the sender’s email directory or list? And if not, which of the following would be a more appropriate time limit?

No, a time limit of greater than 10 days would be more appropriate - it should be 30 days. Many companies who send only a monthly update are hard pressed to work within such a constraint. Also, if you have a situation where your website or server was attacked or shut off, it may take you longer to obtain these files from your provider. There are no rules or regulations for Providers to allow you access to a server that they have shut off, thus forcing non-compliance on this point.

Example from a client: A few weeks ago while sending a federally compliant advertisement to an opt-in list, our provider received spam complaints, and shut down our server that we hosted the websites and delivered the advertisement from, without any warning to us before hand. The opt-in and opt-out service was on that server. We had no access to our files during the shut down. It took 3 to 4 days of communication

back and forth between our provider and us to get the server turned back on, and it was only turned back on if we promised not to deliver our opt-in mailing with it. Thus, we were not allowed to perform within the confines of the law and were also in jeopardy of losing our files, including the email addresses of people who had opted in or out of our lists. We were fortunate to get access to the server at all. This is what I mean by forced non-compliance. Many marketing companies go through this type of ordeal each day on the internet. Often they simply lose their files and all future access to the server. In many instances these companies had remove email addresses on these systems and were unable to take the people off the lists. Later, it is possible that they will be sued for non-removal, however they were never able to get the files. Thus removal of the name becomes an impossibility. This has been an ongoing situation for a number of years. The company that I work for is just one of many has lost its share of ISP provided services where important information such as remove requests, websites etc. could not be retrieved.

#### **D. Identifying additional “aggravated violations”**

Section 5(b) of the Act identifies four “aggravated violations” associated with commercial email:(1) address harvesting; (2) dictionary attacks; (3) automated creation of multiple email accounts; and (4) relay or retransmission through unauthorized access to a protected computer or network.

☒ No - No and address harvesting or dictionary attacks should be taken under study and carefully reviewed. It is rather one-sided. The internet is an open place where all can be. ISPs send web crawlers all over the internet collecting up any and all data, yet a marketer is not allowed to send a web crawler to find publicly displayed email addresses? There should be at least some type of clarification on this part of the law because of this point.

2. Are there new technologies that have been developed or are in development that would contribute substantially to the proliferation of commercial email that is unlawful under § 5(a)?

☒ No, there are no new technologies that I am aware of. Amongst the marketing companies that I am familiar with, the technological focus is on how to get the compliant email delivered while remaining compliant with the law. Again, we have to remember that most marketing companies welcome this law and are more than willing to follow it, but find that it is very difficult to do so when the Internet Service Providers and anti-spamming factions have not had to curtail any of their actions, or be called to task for them.

#### **E.1 Issuing Regulations to Implement Various Aspects of CAN-SPAM -- Defining who is the “sender” of a commercial email message.**

Section 3(16) of the Act defines when a person is a “sender” of commercial email. The definition appears to contemplate that more than one person can be a “sender” of commercial email, for example, an email containing ads for four different companies.

1. Would it further the purposes of CAN-SPAM or assist the efforts of companies and individuals seeking to comply with the Act if the Commission were to adopt rule provisions clarifying the obligations of multiple senders under the Act?

Yes. It is being interpreted in many ways. Most of my clients who are complying with the law have hired me as an attorney to give them guidance. They tell me that the guidance is not even the same from one attorney to the next.

2. If a consumer has “opted out” from receiving commercial email from a particular company, and then receives a subsequent commercial email containing an ad for this company as well as ads for three other companies, does this violate the Act? If so, who has committed the violation?

Other, please specify in the Additional Comments Section at the end of this form. The only violator of the act is the company that sent it a second time after receiving the request for removal.

3. Should the Commission issue regulations clarifying who meets the definition of “sender” under the Act?

Yes

The commission must do two things here. Clarify who meets the definition of the sender and under what circumstances a company is a sender.

Example: One company buys leads for a phone room. Their only transaction is the purchase of leads generated by email marketing. They have no web site; they have no online merchandizing ability -- just when they need leads they buy them. Are they a sender because they bought the leads?

Example 2: Another company has many marketing activities, both on and off the web. They hire an online marketing company to generate hits to their website as one of their marketing activities. This online marketing company sends the email. Who is the sender? The online marketing company that sent the email or the company that is getting the traffic to their website as a result of the emails sent by the online marketing company?

Example #3: A company exclusively and only generates traffic to their website by sending commercial email. They hire others to do this for them. Who is the sender? The companies that actually do the sending or the company that hired them?

## E.2 Issuing Regulations to Implement Various Aspects of CAN-SPAM -- “Forward-to-a-friend” scenarios.

The Act defines “initiate” to mean originate or transmit, or procure the origination or transmission of a message. In turn, the term “procure” means to pay, provide consideration, or induce a person to initiate a message on one’s behalf.

3. Should these marketing campaigns have to comply with the Act, and if so, who should be considered a person who “initiates” the message when one person forwards the message to another person?

No, these types of marketing campaigns should not have to comply with the Act. Here we have a very common scenario. I receive an email from a political group, they brief me on something and tell me to send this to as many people as I know. If I believe in that cause, I'm going to send it. If I don't, I'm not going to send it.

Or, I receive an ad promoting a travel club. I am excited. I send it to my friends. Perhaps I am thinking "hey maybe we can all join and travel together".

These two examples are in no way instances of people who are in violation of the can spam act and if we get any heavier into regulation than we already are, we are going to regulate people out of using email all together.

Certainly any forwarded message should carry the original opt-out mechanism with it, and it should be the responsibility of the originating company to maintain their opt-out mechanism to handle any forwarded messages.

4. Who should be required to provide an “opt-out” mechanism for such a message?

Other, please specify in the Additional Comments Section at the end of this form. No, opt-out would be required by a forwarding party. The opt-out should be required only by the advertising company that originally delivered the advertisement, and should be in the email forwarded.

8. Should unsolicited commercial email campaigns that rely on having customers refer or forward the email to other parties be treated differently from other unsolicited commercial email? Yes. All companies rely heavily on their happy customers to spread the word of their products or services. It is no different for email advertisers. The people who refer or forward for them should not be classified under this act.

Yes

### **E.3 Issuing Regulations to Implement Various Aspects of CAN-SPAM –The inclusion of a “valid physical postal address”.**

Section 5(a)(5)(A)(iii) requires the disclosure of “a valid physical postal address of the sender” in each commercial electronic mail message.

2. Should a P.O. Box be considered a “valid physical postal address”?

Yes- **There are still a number of US locations that do not have street addresses.**

2. Should a commercial mail drop be considered a “valid physical postal address”?

**Yes. The postal address is for the purposes of reaching the sender. The sender can be reached at a PO Box just as easily as a street address.**

**The major concern here is safety. Advertisers do not want their employees attacked by the anti-spamming groups, or other crazy individuals. Although they should be contactable through postal services, they should be able to be allowed the safety of not having to list their actual physical location.**

**Further in many instances people are running small internet businesses from their homes and do have families to protect as well. All of these are valid issues for companies choosing PO boxes or mail drops. They are still reachable, but people cannot simply drop by and attack them.**

**A good analogy to our safety concerns would be abortion clinics. Certainly, no one would ask Doctors who perform abortions to list their home addresses for the world to see, the pro-life people have already murdered enough Doctors. The emotional response by anti-spammers is as great as those of the pro-life factions, and many of my clients have received death threats.**

### **E.4 Issuing Regulations to Implement Various Aspects of CAN-SPAM -- Information in a message’s “from” line.**

1. Is the Act sufficiently clear on what information may or may not be disclosed in the “from” line, pursuant to Section 5(a), including the kind of “from” line information that should be considered acceptable under the Act?

**No it is not. There is still much confusion about company name, employee name, individual name, company title, etc. This area needs much clarification.**

2. If a sender’s email address does not, on its face, identify the sender by name, does that email address comply with § 5(a)(1)? **Yes. It is very rare that an individual**

can obtain an email address that actually identifies them or their company. If the email does work and can send and receive email then that has to be sufficient.

Again, the purpose of the from is the ability to reach the sending party, and not the identity of the party. As long as the from address is a working e-mail address by which the sending party can be reached the purposes of the act is fulfilled.

### **The Implementation of a National Do Not Call Registry.**

Currently I have a client who owns the National NoMoreEmail system, earlier known as RemoveMe.Com. This system allowed internet users to enter their name into a database. Marketing companies could then upload their lists which would be cleaned of all e-mail addresses in the database. The beauty of this system is that the list of opt-outs are not given to the marketing companies.

During the time that the system was available, the client managed to add more than 50 million email addresses (these people added themselves to the removeme.com database in the early days when mailers were allowed to add a link in the advertisement they were sending out so that people could remove themselves).

Unfortunately, the system is hardly known about, not used often and has been subject to denial of service attacks on several occasions. The purpose of these attacks is to bring the system offline. Due to this situation, the system has been offline for the past 8 months. The attacks of course, are the work of anti-spammers who attempt to eliminate all commercial email advertising and related services from the net.

**The major benefit** to this registry could be that it finally provides a place where all ISPs, backbones, individuals, etc. can put email addresses of people who do not want to receive email advertisements, thus quieting down the internet to a major degree. The majority of the problem with complaints right now is that a Marketing Company who has the email address in their list has no way of knowing (because the ISPs do not release the information of the complaining email address to the marketing company) who to remove from their list. The ISP does not tell their customer (the marketing company) who to remove due to privacy issues or concern that the marketing company won't actually remove it anyway. (Another common statement that is not correct. Marketing companies are plagued by people who they cannot get out of their lists, these are unwanted by the marketing company because they put undue stress on their systems, often bring massive attacks against their systems and cause the company to lose income) These problems could be completely solved in short order. ISPs and backbones can add complainers to the registry, and marketing companies will be able to get those names off their lists. Everything then starts to calm down.

**The implementation of a system for rewarding those who supply information about CAN-SPAM violations.**

This is going to bring undue pressure and heat first against the FTC as they come to know all the crazy people in the anti-spam factions of the internet. And it is going to open the door to some very serious problems. Already there is a big problem with criminals who are well-known anti-spammers running rampant over the Internet Service Providers – please see this link for research done on one of the owners of spamhaus:  
<http://www.optinbig.com/jr/>

Here are some links for the well-known anti-spammer Shiksaa – Susan Wilson:  
I am sure you will find that her manner is unacceptable as well.

- <http://members.aol.com/alexeypanovspams/>
- [From: shiksaa Newsgroups: news.admin.net-abuse.email Subject ...](#)
- <http://www.cm.nu/~shane/lists/comp.mail.sendmail/2001-06/0092.html> - here she openly states she can start making trouble for an ISP if they anger her.
- <http://groups.google.com/groups?q=Shiksaa&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=7%24--%25%24%25-%25%24--%25-%25-%24%40news.noc.cabal.int&rnum=2>
- <http://groups.google.com/groups?q=Shiksaa&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=2%24--%25%24%25%24--%25-%25-%24%40news.noc.cabal.int&rnum=5>
- This is a post of her contact information:  
<http://groups.google.com/groups?q=Shiksaa&start=10&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=202cccc5.0304301952.46b3db58%40posting.google.com&rnum=14>

These are just a few links that show her attitudes, actions, and conversations against those whom she believes are guilty of spamming. She, and people like her, have damaged many with false reports and innuendos. Their method of operation is intimidation, threats, and blocking. ISPs are more often than not forced to bow to their demands.

Currently one ISP is suing another because of such actions; here is a letter from just a few days ago (reprinted with permission):

OptinRealBig.com, LLC

To Our Valued Customers:

As most of you are aware, Spamhaus has taken it upon themselves to try and put our company out of business by threatening and intimidating ISP's that we work with to not provide us with bandwidth. Recently, Spamhaus threatened to place Wiltel's corporate email servers on the Spamhaus Blocklist if Wiltel allowed Optigate to service OptinRealBig.com, LLC or WholesaleBandwidth. Wiltel demand that Optigate terminate its services to Optin and Wholesale, and Optigate refused, on the basis that neither company was in violation of any law or Optigate's AUP. Although, we don't know all the facts at this time, apparently Spamhaus carried through with their threat.

On March 22, 2004 Witel Communications, LLC ("Witel") located in Tulsa, Oklahoma filed in the United States District Court for the Northern District of Oklahoma, a Verified Complaint and Application for Temporary Restraining Order ("TRO") against Optigate Networks, Inc., whose offices are located in Oakhurst, California.

Witel requested in its TRO that the Court order Optigate from directly or indirectly transmitting or sending unsolicited bulk email directly or from any of its customers, including but not limited to, OptinRealBig.com, LLC and WholesaleBandwidth.

On March 24, the matter came before Chief Judge Holmes, and after listening to testimony from counsel for both Witel and Optigate, the Court denied the Application for a TRO. The Court ordered the parties to appear before him on April 22, 2004 for a Preliminary Injunction hearing. The Court also ordered that Witel provide Optigate with evidence to support Witel's allegations that its Optigate was under a contractual obligation to comply with Witel's Acceptable Use Policy that defined spam in narrower terms than the Can-Spam Act of 2003. I can also tell you that the Court referred to Spamhaus in terms that no one would consider endearing.

I want to assure you that neither Spamhaus, Witel, nor any other organization is going to put us out of business because of the services that we provide our customers. Our attorneys are confident that our company is in complete compliance with all Federal and state statutes, and constantly monitor our services and conduct to ensure that we stay in compliance.

It is important for you to understand that all we ask of Spamhaus and its friends is that they report accurate information rather than innuendos and gossip. Their inaccurate reports are harmful to both legitimate internet marketers and their Internet Service Providers.

We do offer an alternative to the current Spamhaus listings that interfere with your website hosting. You can host with us and not worry about being harassed by Spamhaus and your ISP. We will take the harassing communications from Spamhaus.

If you have any questions or concerns regarding these issues please do not hesitate to contact me.

Sincerely,

Scott Richter, President  
[Scott.richter@optinbig.com](mailto:Scott.richter@optinbig.com)

These are the people your program is most likely to reward.

Further and of a more urgent nature is the fact that advertisers who are following the law are now having to contend with the situation that their websites or ads are being copied and then used in non-compliant emails. People like Shiksaa have no right to be allowed to investigate and persecute companies or groups who are suffering from these new attacks, and they should not be rewarded for their malicious actions.

### **The Effectiveness and Enforcement of the CAN SPAM Law.**

The major drawback to the enforcement of the CAN SPAM law is that the lack of a Can-Spam compliant certification. There is no routine set up that allows a company to notify the FTC they are in compliance with the law, or even allow them to file a report that shows its websites, advertisements and company information so that they can work in peace.

As marketers, they are dealing with ISPs who shut down their services despite the fact that they are in compliance, and anti-spammers who attack, report them, or attempt to cause them to lose their services despite their compliance.

The marketers have no recourse. Two weeks ago, an anti-spammer or some unknown entity claimed that a client's company info at the registrar was incorrect. It was not, yet they had to deal with clearing their name, and proving their innocence. They were never able to find out who claimed their information was incorrect. They have to deal with these types of situations on a routine basis. IP addresses are shut off for spamming despite compliance, Opt-In mailings are treated the same as non-opt-in mailings. It seems that some days our clients spend more time trying to clear their names, actions etc. than actually working.

Enforcement would be much easier all the way around if marketers could sign up with a certifying body, and send their website links and advertisements to the certification authority prior to any email being sent.

The majority of people who market on the internet are just business people engaged in promotion. They do not like being attacked and work to remain anonymous not because they are fraudulent, but rather because of anti-spammers like Shiksaa.

The real issue in requesting such a system is that many marketing companies feel that it would just allow them to be sued that much faster and would prefer not to have such a system. In part this situation arises because most of the Internet Service Providers have not or will not alter their TOS/AUP agreements to allow for federally compliant advertising. Until this is done, Marketing companies run the risk of being sued despite their compliance. That in itself would be tolerable, except that insurance companies do not offer business insurance policies to internet marketing firms due to the high risk that they present.

In essence something somewhere has to give for successful compliance and enforcement on all sides.

## Subject Line Labeling

There is nothing most Marketing Companies would like more than to use a single catchy and snappy subject line that really interest the consumer in their product and get the email advertisement opened without the need for any subterfuge. However, due to the fact that subject lines are heavily filtered (like from names and email addresses and IP addresses) by the Internet Service Providers and anti-spamming groups, they resort to innocuous subject lines.

The problem is that most of the federally compliant email is actually trapped by the filtering of ISPs. Compliant companies are struggling to remain within the confines of the law and get their advertisement delivered as well. And I believe a recent lawsuit filed by one of the major ISPs illustrates this point nicely: It goes so far as to list as a part of the suit that the subject line contained an additional list of letters after the subject itself, to help pass through their filters. The CAN SPAM law of 2003 is clear that the subject must not be misleading, it does not claim that the subject line must not outwit a filtering system- yet there is already a lawsuit on the books with this as a part of it. Suits that have items like this as a part of them are very intimidating to federally compliant companies.

### Other Issues:

There is a new problem cropping up for Marketing Companies now. This link shows a company that filters and adds marketing companies that involve themselves in email marketing to common RBL lists. <http://www.joewein.de/sw/jwSpamSpy/index.htm>

Here is a quote from that site:

“Most spam is sent using fake addresses. By including these addresses in a blacklist you would end up blocking legitimate mail. Our list is different: **We try to list only genuine spam domains that either have been advertised inside spam or have been registered by notorious spammers.** Get a free subscription to receive additions by e-mails!”

As you can see, one action of the filtering software is to check the company name on the registrar information of the domain. Keep in mind that anti-spammers are not selective in who they label as a notorious spammer. This will or maybe already is causing companies to have to set up under new names simply to avoid the RBL listings, which cause their advertisements to get blocked.

I do not expect that it will be long before the fact that marketing companies have to consistently create new company names/info etc. for themselves also gets labeled as some type of act to hide illegal actions. Which as usual, may be true for one or two percent of the industry, but not the industry at large.

So much of what the Marketing Companies are dealing with is actually not covered by the law. And although the law provides guidelines and penalties, the real issues that the companies are confronted with remains how to advertise successfully despite the fact that

people who do not want to receive their advertisements remain hidden in their lists and form groups that use threats and coercion against the companies and the internet service providers to eliminate all email advertising instead of just remove themselves from the lists.

A US company to successfully get through the filters and avoid the anti-spamming groups will have to do one or all of the following during the course of a month.

- **Create a new company** – to resolve the issues of company names in domains being blacklisted.
- **Purchase new domains** – to resolve the issues of ISPs blocking their domains or having their domains blacklisted. To stop attacks launched against the IP address by anti-spamming groups or individuals who are trying to remove their sites from the web.
- **Obtain new IP addresses** – to resolve the issues of blocking, shut off and blacklisting. To stop attacks launched against the IP address by anti-spamming groups or individuals who are trying to remove their sites from the web.
- **Create or obtain new from addresses** – to resolve the issue that their current from address is now blocked by filtering.
- **Redevelop new subject lines** – to resolve the issue that their current subject lines are now blocked by filtering.
- **Redevelop new removal information** – to resolve the issue that their current removal links or statements are now blocked by filtering.

These companies will be and are accused of performing or engaging in illegal activities which is “supported by their actions” but the fact of the matter is that the majority of these companies are engaged in nothing more than valid advertising that does comply to the law, but also must get through filtering by the ISPs and protect them against attacks from the anti-spamming groups.

Respectfully submitted for your consideration on March 30, 2004