

1 Douglas E. McKinley, Jr.  
2 PO Box 202  
3 Richland WA, 99352  
4 (509) 628-0809

THE HON. JOHN C. COUGHENOUR

5 MERKLE SIEGEL & FRIEDRICHSEN, P.C.  
6 Robert J. Siegel  
7 1325 Fourth Ave., Suite 940  
8 Seattle, WA 98101  
9 (206) 624-9392

10 UNITED STATES DISTRICT COURT  
11 WESTERN DISTRICT OF WASHINGTON, SEATTLE

12 **JAMES S. GORDON, Jr., a married**  
13 **individual, d/b/a**  
14 **'GORDONWORKS.COM',**

**NO. CV06-0204JCC**

**Plaintiff,**

v.

**PLAINTIFFS' MOTION FOR  
PARTIAL SUMMARY JUDGMENT**

16 **VIRTUMUNDO, INC, a Delaware**  
17 **corporation, d/b/a**  
18 **ADNOWLEDGEMAIL.COM;**  
19 **ADKNOWLEDGE, INC., a Delaware**  
20 **corporation, d/b/a**  
**ADKNOWLEDGEMAIL.COM;**  
**SCOTT LYNN, an individual; and**  
**JOHN DOES, I-X,**

**Defendants.**

21  
22  
23  
24  
25  
PLAINTIFFS' MOTION FOR PARTIAL SUMMARY  
JUDGMENT  
GORDON v. VIRTUMUNDO GROUP, INC., ET AL.

**MERKLE SIEGEL & FRIEDRICHSEN**  
1325 Fourth Ave., Suite 940  
Seattle, WA 98101  
Phone: 206-624-9392  
Fax: 206-624-0717

**The Relevant Facts**

1  
2 The material facts of this matter are uncontested. Defendant Virtumundo is a large,  
3 highly successful, privately held corporation whose primary business consists of sending billions  
4 of commercial electronic mail messages over the internet (hereafter “commercial emails,”  
5 “emails”, “spam emails,” or “spam”) to hundreds of millions of people throughout the United  
6 States and the world.<sup>1</sup> The Wall Street Journal estimates that by sending this massive volume of  
7 spam Defendant Virtumundo generates annual revenues as high as one hundred million dollars  
8 (\$100,000,000.00).<sup>2</sup> Approximately 13,000 of Defendants’ spam were received by a small  
9 Internet Access Service located in Washington State owned and operated by the Plaintiffs, James  
10 S. Gordon Jr. and Omni Innovations (hereafter collectively “Gordon”). 7,890 of these emails  
11 form the basis of this motion.<sup>3</sup>  
12

13 The information the Defendant placed in the “From” line of these emails does not  
14 accurately identify the sender of the emails. Instead, the Defendant placed ambiguously worded  
15 advertising copy in the “From” line of the header, followed by an ambiguous email address that  
16 provides no further indication of the actual name of the sender. When received by a typical  
17 email user, only the advertising copy is shown, and the recipient has no way of knowing who  
18 sent the email without opening it. These emails, showing this header information, are set forth as  
19

---

20 <sup>1</sup> Defendant Virtumundo estimated at depositions that it sends up to 1.5 billion emails per month  
21

22 <sup>2</sup> The Defendants have declined to state their income, however, the press has set forth this  
estimate. See <http://kansascity.bizjournals.com/kansascity/stories/2001/12/31/story2.html>

23 <sup>3</sup> The Plaintiff realizes that the Plaintiff has been inconsistent in setting forth the total number of  
24 spam sent by the Defendants. The Declaration of James S. Gordon, Jr. sets forth the reasons for  
these inconsistencies.  
25

1 Exhibit A to the declaration of James S. Gordon, Jr. filed concurrently herewith (hereafter the  
2 “Gordon declaration”). Examples of the complete “from” line from these emails include the  
3 following:

4 **From: “Criminal Justice” <CriminalJustice@vm-mail.com>**

5 **From: “Public Safety” <PublicSafetyDegrees@vadmin.com>**

6 **From: “Trade In” <TradeIn@vm-mail.com>**

7  
8 In each of these emails, as is the case with all 7,890 emails at issue here, no actual  
9 sender is identified in the “From” line in any meaningful sense.

10 **The Issue Before the Court**

11 The Plaintiffs’ contend that the information Defendants place in the “From” fields of  
12 these commercial emails violates the ‘Controlling the Assault of Non-Solicited Pornography and  
13 Marketing Act (15 U.S.C. 7701, et seq., Public Law No. 108-187, (hereafter “the Act” or “the  
14 CAN-SPAM ACT”), and the Washington State’s Commercial Electronic Mail Act, (RCW  
15 19.190 et seq. (hereafter “CEMA”) because a typical user is unable to identify the sender of the  
16 email without opening the email. Accordingly, this motion presents the following question of  
17 statutory interpretation:  
18

19 *Does a commercial electronic mail message that does not accurately identify the sender of the*  
20 *email in the “From” field of the header comply with the CAN SPAM Act and/or CEMA?*

21  
22 On first impression, this may appear to be a trivial question. It is not. The internet, and  
23 specifically email, is rapidly becoming the preferred and most utilized mode of communication  
24 in the U.S. for both commercial and personal purposes. Not coincidentally, the spam industry  
25

1 has become pervasive, both in its size and in its impact. Other Courts have noted that the cost of  
2 spam to the US economy is substantial; “deleting unwanted email costs nearly \$22 billion in lost  
3 productivity.” *MaryCLE, LLC v. First Choice Internet, Inc.*, 166 Md.App. 481, 890 A.2d 818,  
4 836 (Md. Spec. App. Jan. 26, 2006). The Court’s ruling in this case will determine how multi-  
5 million dollar email marketing corporations like the Defendants must address the trillions of  
6 emails they send to the general public. This, in turn, will determine how these trillions of emails  
7 will appear in the inboxes of hundreds of millions of email users throughout the United States.  
8 Since the Court’s ruling will clarify both the Federal and State standard for how the “From” line  
9 of these spam emails is displayed to the American public, the Court’s ruling will determine the  
10 amount of time and effort hundreds of millions of email users will have to expend to accurately  
11 distinguish between the flood of unwanted commercial emails that they wish to delete and/or  
12 filter from their inboxes, and the vastly smaller volume of non-spam email messages which the  
13 recipient actually wants to open and read as part of their private and professional lives.

15 While the time and energy associated with each of these individual decisions may be  
16 small, cumulatively the time and expense is monumental. The sheer size of the spam industry,  
17 and the massive volume of the spam that it generates, insures that even seemingly  
18 inconsequential differences in how easily spam can be identified and deleted by the recipient add  
19 up to enormous amounts of time and money wasted doing so. National surveys have shown that  
20 22.9 million hours a week are wasted on Spam. *Id.* at 836. Thus, the Court’s ruling determine  
21 whether the US economy endures billions of dollars in wasted time and lost productivity, an  
22 economic impact that will dwarf the amount in dispute between these parties.

1 **Legal Standard**

2 A court should grant summary judgment when "there is no genuine issue as to any  
3 material fact and the moving party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56.  
4 A court must regard the evidence in the most favorable light to the nonmoving party. *Seabulk*  
5 *Offshore, Ltd. v. Am. Home Assurance Co.*, 377 F.3d 408, 418 (4th Cir.2004). Once a summary  
6 judgment motion is properly made and supported, the opposing party has the burden of showing  
7 that a genuine dispute exists. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574,  
8 586-87 (1986). There are no material facts in dispute, and this case is ripe for summary judgment  
9 as to the issues presented here.

10 **Argument**

11 Avoiding billions of dollars of lost productivity is not a sufficient reason alone for the  
12 Court to rule that the CAN SPAM Act and CEMA require spam to accurately identify the person  
13 who sent the email in the "From" field of the header. Rather, the Court should hold that  
14 substituting the name of the "person who initiated" the email for advertising copy in the "From"  
15 field of the header violates the CAN-SPAM Act and CEMA because that was the clear intent of  
16 Congress and of the Washington State legislature in enacting the respective statutes.

17 **THE CAN-SPAM ACT**

18 The CAN SPAM statute demonstrates conclusively that the accurate identification of the  
19 actual sender of a commercial electronic mail message in the "header" portion of that email is  
20 both required under, and central to, Congress' scheme to regulate commercial email. A "header"  
21 is defined at 15 USC 7702(8):  
22  
23  
24  
25

1 (8) HEADER INFORMATION- The term 'header information' means the source,  
2 destination, and routing information attached to an electronic mail message, including the  
3 originating domain name and originating electronic mail address, and any other  
4 information that appears in the line identifying, or purporting to identify, a person  
5 initiating the message. (emphasis added)

6 While the definitions section of the Act does not define the term "from line," 15 USC  
7 7704(a)(1)(B) provides that:

8 (B) a 'from' line (the line identifying or purporting to identify a person initiating the  
9 message) that accurately identifies any person who initiated the message shall not be  
10 considered materially false or materially misleading; (emphasis added).

11 Taken together, these definitions demonstrate Congress' understanding that the "From"  
12 line in a "header" is used to "identify a person initiating the message." The convention that the  
13 "From" line is to be used to identify the person who sent the email is thus explicit in the Act, and  
14 is entirely consistent with the everyday experience of millions of email users. Assuming  
15 arguendo, that "person" is understood to include entities such as the Defendant corporation, the  
16 fact that Defendant Virtumundo here failed to identify itself in the "From" line, but instead  
17 falsely displayed its identity as advertising copy, is indisputable.

### 18 "From" Lines in E-Mail Headers

19 To fully appreciate the Congressional intent behind the Act, and why the Defendant's  
20 conduct violated the Act, it is helpful to have a more detailed understanding of how a "From"  
21 line actually operates. A useful explanation has been provided by the email marketing industry  
22 itself. Roving Software Incorporated, d/b/a Constant Contact, describes itself as "the leading  
23 provider of email marketing services to small businesses, associations, and nonprofits." As  
24 explained by Constant Contact on their website, the "From" line in the header has two parts:  
25



1 Part one is the "From Name" - the name, such as "Constant Contact's Email Marketing Diva,  
2 Michelle Keegan" also identified in some programs as the "Sender." Part two is the "From  
3 Address" - the electronic address including "@" such as, tips@constantcontact.com.<sup>4</sup> As  
4 explained by Constant Contact, "Your recipients may see just the From Name, just the From  
5 Address, or both depending on their email client or reader."

6 Thus, there are two parts to the "From" line portion of the header referenced at 15 USC  
7 7704(a)(1)(B); the "From name" which should identify the name of the actual person or entity  
8 who sent the email, i.e., the sender, and the "From address" which is the return email address of  
9 the sender. These two bits of information can be distinguished by their function, and by their  
10 intended audience. The "From name" of the sender is entirely informational, and exclusively  
11 directed to human beings. The only proper function of the "From name" is to inform a human  
12 recipient of the true identity of the sender. The "From address," on the other hand, is primarily  
13 functional. It provides an address for a reply email, and is written using the syntax used by  
14 computers to route email across the internet. The "From address" is thus information that is  
15 primarily used by computers. The "From name" can thus be distinguished from the "From  
16 address" because the only purpose of the "From name" portion of the "from line" is to display,  
17 and thereby reveal, the name of the actual sender to the human being who receives the email  
18 without the recipient having to actually open the email. The Court should note that, unlike the  
19 spam Defendant sent to Gordon, the headers in internal Virtumundo corporate email that  
20  
21 Virtumundo employees use to send email to and from one another correctly include the name of  
22

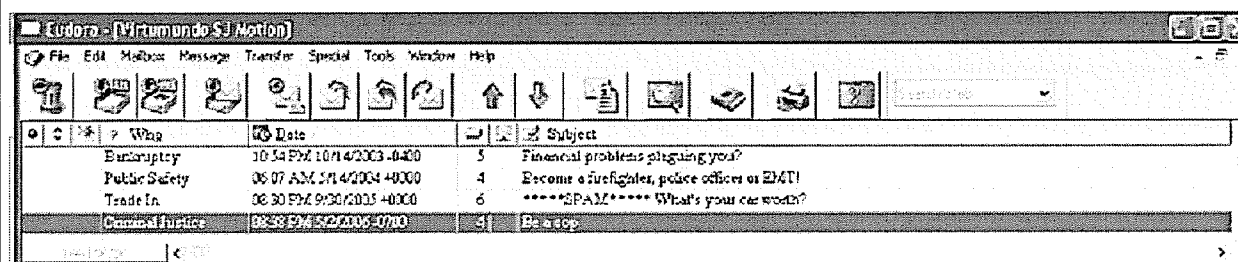
---

23  
24 <sup>4</sup> <http://www.constantcontact.com/learning-center/hints-tips/volume7-issue5.jsp>

1 the actual person who sent the email in the “from name” field, so that the recipient will know  
 2 who it is from without having to open it. (See Exhibit B to Gordon Declaration). This is  
 3 typically the case with emails sent by and between individuals and entities when they are not  
 4 trying to hide their identities.

### 6 Displaying “From Lines” in Email Programs

7 The significance of the “From name” and “From address” to the spam industry lies in  
 8 how this information is displayed to an email recipient. As set forth in the Gordon Declaration,  
 9 it is typical for an email recipient to see only the “From name” portion of the header, and not the  
 10 “From address” portion. In the instant case, only the “From name” portion of the emails were  
 11 displayed to Mr. Gordon by his email program, Eudora, as shown in Exhibit C of the Gordon  
 12 declaration. As seen in the exhibit and the example below, Gordon’s email program only  
 13 displays the “From name” portion of the header in the “who” field, and does not display the  
 14 “From address” portion at all.



21 Gordon’s view of these emails is typical. Most email programs display only the “From name”  
 22 portion of the header, and do not display the “From address” portion at all. (Paragraph 18  
 23 Gordon declaration). Gordon’s declaration is buttressed by an article published June 2, 2003,  
 24 during the months leading up to Congress’ passage of the Act, where email marketer  
 25 “EmailLabs” provided a chart of the main email clients, and how those email clients displayed



1 the “From name” and the “From address.” (Exhibit D Gordon declaration)<sup>5</sup> As shown in the  
2 EmailLabs chart, each and every email client in use at the time, with the sole exception of AOL,  
3 displayed the “from name” either exclusively, or at least first, in the email client inbox.

4 There is also no doubt that the email marketing industry was and is keenly aware of the  
5 importance of the “From name” in getting their emails opened. An industry publication article  
6 from Constant Contact opens with the following quote:

7 According to the DoubleClick Consumer Email Study released in late 2002, 60% of  
8 respondents cite the “From” line as the most important factor motivating them to open  
9 emails, while 35% cited the "Subject" line.

10 (See Gordon declaration Exhibit “E”)

11 The EmailLabs article (Gordon declaration Exhibit “D”) agrees, stating:

12 Among the many challenges of distributing email newsletters and campaigns are the  
13 varying ways that email clients render your From and Subject lines. Why is optimizing  
14 the From and Subject lines so important? It's simple, really. The From line is what  
15 recipients use to determine whether to delete an email. The Subject line is what  
16 motivates people to actually open the email.

### 17 **Congressional Recognition of the “From Line” Portion of the Header**

18 It is clear from the legislative history that Congress understood the significance of the  
19 “From name” portion of the header, and the distinction between the “From name” and the “From  
20 address.” It is also clear that Congress intended that the Act compel the sender to accurately  
21 identify themselves in the header of the email, beyond simply providing an ambiguous return  
22 email address, regardless of whether such address may actually be registered to the otherwise  
23 disguised sender.

24 <sup>5</sup> [http://www.emaillabs.com/email\\_marketing\\_articles/article\\_optimizeforclients.html](http://www.emaillabs.com/email_marketing_articles/article_optimizeforclients.html)

1 “If enacted, S. 877 would require senders of all commercial e-mail to include a valid  
2 return e-mail address and other header information with the message that accurately  
3 identifies the sender and Internet location from which the message has been sent.” Sen.  
4 Rep. No. 108-102, at 7 (2003) (emphasis added).

5 Thus, the importance of the “From” line to both email marketers, and the Congressional  
6 scheme to regulate email marketers, cannot be overstated.

7 For commercial email to achieve its intended result, it first must be received by a  
8 recipient. As a result, a virtual arms race has developed between the email marketers, sometimes  
9 known as “spammers” and their targets, with the spammers continually developing ever more  
10 nefarious ways to circumvent spam filter countermeasures. Once a spam has reached a targeted  
11 email inbox, it is critical that the spammer induce the recipient to actually open and read the  
12 spam email. Tricking recipients into actually clicking on, and thereby opening spam, is a critical  
13 skill for a successful spammer. Thus, the information in the “From name” is critical to  
14 preventing a recipient from deleting the spam, and then enticing the recipient to open it.

15 The vast majority of e-mail users decide whether to read the email message, or to delete it  
16 as spam, based only upon two pieces of information: the “from name” and the subject line. For  
17 the spammer hoping to have their email opened and read, these two fields in a spam header  
18 represent their only opportunity to convince the target to open it and read it. It is no surprise that  
19 sophisticated, multi-million dollar spammers like the Defendants here would not want to waste  
20 this valuable space revealing their actual identity. Instead, they use that space to falsify their  
21 identity by replacing it with advertising copy. The only surprise is that the Defendants think they  
22 can convince the Court that doing so is legal.  
23  
24  
25

**Congress Did Not Intend to Force Consumers To Open Spam**

1  
2  
3 Congress explicitly recognized the importance of providing email recipients with  
4 information necessary to accurately identify the sender and the subject of commercial email  
5 without having to open unwanted spam emails to find this information. 15 USC 7701(b)(2) &  
6 (3) explicitly sets forth the Congressional intent for the Act:

7 “the Congress determines that ... senders of commercial electronic mail should not mislead  
8 recipients as to the source or content of such mail” (emphasis added)

9 15 USC 7701(a)(7) & (8) recites the Congressional findings upon which this intention is based:

10 (7) Many senders of unsolicited commercial electronic mail purposefully disguise the  
11 source of such mail.

12 (8) Many senders of unsolicited commercial electronic mail purposefully include  
13 misleading information in the messages' subject lines in order to induce the recipients to  
14 view the messages. (emphasis added).

15 Congress thus explicitly recognized in the Act that part of the problem with the spam  
16 industry was that spammers used deception to induce recipients to open emails that they would  
17 not otherwise open. Congress further articulated the reasons for Congress' concern that  
18 consumers were being forced or tricked into opening spam messages in the legislative history of  
19 the Act.

20 “The inconvenience and intrusiveness to consumers of large volumes of spam are  
21 exacerbated by the fact that, in many instances, the senders of spam purposefully disguise  
22 the source or content of the e-mail by falsifying or including misleading information in  
23 the e-mail's “From”, “reply-to”, or “subject” lines. Thus, the recipient is left with no  
24 effective ability to manage the constant inflow of spam into an e-mail inbox because he  
25 or she cannot often tell without opening the individual messages who is sending the  
messages or what they contain...” Sen. Rep. No. 108-102, at 3 (2003) (emphasis added).

1 “Furthermore, headers continued to be falsified, not only to trick ISPs' increasingly  
2 sophisticated spam filters, but also to lure consumers into mistakenly opening messages  
3 ...” *Id.* at 3. (emphasis added).

4 “Additionally, many spam messages contain "Web bugs" or other hidden technological  
5 mechanisms to immediately notify spammer via the Internet with an unsolicited message  
6 has been opened. Far short of replying to a spam message, a consumer's mere act of  
7 opening a spam message containing a web bug may eventually cause that consumer to  
8 receive more spam as a result of confirming to the spammer his or her willingness or  
9 susceptibility to open unsolicited e-mail.” *Id.* at 4. (emphasis added).

10 Congress also provided reasons for the policy of forcing spammers to identify themselves  
11 without requiring a recipient to open their email directly in the Act. For example, 15 USC  
12 7701(a)(5) notes:

13 “Some commercial electronic mail contains material that many recipients may consider  
14 vulgar or pornographic in nature.”

15 Plainly, Congress was trying to provide the public with a way to identify pornographic  
16 and vulgar emails without having to open them.

17 “In its recent report, the FTC found that more than 40% of all pornographic spam either  
18 did not alert recipients to images contained in the message or contain false subject lines,  
19 thus "making it more likely that recipients would open the messages without knowing  
20 that pornographic images will appear." Unsuspecting children who simply open e-mails  
21 with seemingly benign subject lines may be either a front-end with pornographic images  
22 in the e-mail message itself, or out automatically and instantly taken - without requiring  
23 any further action on their part (like clicking on a link) - to an adult webpage exhibiting  
24 sexually explicit images.” Sen. Rep. No. 108-102, at 4 (2003) (emphasis added).

25 Congress had good reasons to protect the public from being tricked into opening spam  
26 emails in addition to unwanted exposure to vulgarity and pornography. Opening email from an  
27 unknown source carries a substantial risk. In addition to the “web bugs” Congress discussed in  
28 the legislative history, email is a primary means by which malicious computer viruses are

1 distributed. Opening an email message from an unknown source can have catastrophic  
2 consequences. Malicious viruses carried by spam emails can not only destroy an unsuspecting  
3 recipient's computer by causing it to "crash", but can also hijack the recipient's computer to  
4 replicate and send out copies of themselves to all of the recipient's contacts. The mere act of  
5 opening malicious emails has resulted in untold damages to computer resources worldwide.  
6 (Exhibit F to Gordon Declaration). It is notable, perhaps, that one of the most well known and  
7 destructive viruses in 2005 was actually named after Defendant "VirtuMundo." (Exhibit G to  
8 Gordon Declaration). Given the notoriety of this virus, it is perhaps understandable that these  
9 Defendants do not want to identify themselves in their "From" lines. But that doesn't make it  
10 legal.

11  
12 Congress explicitly recognized that the mere act of reviewing and discarding the  
13 tremendous volume of spam email imposes a significant cost on the economy, even if that spam  
14 does not contain malicious computer viruses and pornography. At 15 USC 7701(a)(2), (3) & (4)  
15 the Act recites the Congressional findings:

16 (2) The convenience and efficiency of electronic mail are threatened by the extremely  
17 rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited  
18 commercial electronic mail is currently estimated to account for over half of all electronic  
19 mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise.  
Most of these messages are fraudulent or deceptive in one or more respects.

20 (3) The receipt of unsolicited commercial electronic mail may result in costs to recipients  
21 who cannot refuse to accept such mail and who incur costs for the storage of such mail,  
or for the time spent accessing, reviewing, and discarding such mail, or for both.

22 (4) The receipt of a large number of unwanted messages also decreases the convenience  
23 of electronic mail and creates a risk that wanted electronic mail messages, both  
24 commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger

1 volume of unwanted messages, thus reducing the reliability and usefulness of electronic  
2 mail to the recipient. (emphasis added).

3 Thus, there can be no question that Congress intended to force email marketers to provide  
4 email users with accurate identifying information that would allow them to minimize “the time  
5 spent accessing, reviewing, and discarding” unwanted email. Congress explicitly recognized that  
6 commercial electronic mail was purposefully designed to “induce the recipients to view the  
7 messages.” Congress also explicitly recognized that “most of these messages are fraudulent or  
8 deceptive in one or more respects” and that they “create a risk that wanted electronic mail  
9 messages... will be lost, overlooked, or discarded amidst the larger volume of unwanted  
10 messages.” Accordingly, it is beyond dispute that one of Congress’ goals for the regulatory  
11 scheme set up by the Act was to require the sender of commercial emails to provide header  
12 information that would allow email users to immediately and accurately recognize the actual  
13 identity of the sender of the email and the subject *without having to take the time and energy to*  
14 *actually open the unwanted spam emails*. Consequently, Congress achieved this goal the only  
15 way that it could, by regulating the only part of the email that a recipient could view without  
16 opening the email: the content of the headers.  
17

18  
19 **Congress Intended to Force Email Marketers To Accurately Identify Themselves in the**  
20 **Header Information**

21 The requirement is set forth at 15 USC 7704(a)(1):

22 (a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES-

23 (1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION

24 INFORMATION- It is unlawful for any person to initiate the transmission, to  
25 a protected computer, of a commercial electronic mail message, or a



1 transactional or relationship message, that contains, or is accompanied by,  
2 header information that is materially false or materially misleading...

3 If the Court accepts the premise that Congress intended and assumed that the "From  
4 name" field is supposed to be used to accurately identify the sender of an email, it becomes  
5 indisputable that the information provided by the Defendants in their "From name" fields is false  
6 and deceptive. Under the Act, the only information that could be used in a "From name" field  
7 that would not be false is the actual, accurate identity of the person or entity who actually sent  
8 the e-mail, or perhaps the actual, accurate identity of the person or entity who hired the  
9 Defendant to send the email on their behalf. But here, the information Defendant put in the  
10 "From" field does not identify any person or an entity at all. The information provided by  
11 Defendant is therefore false by definition.

12  
13 **Header Information Is "Materially False Or Misleading" If It *Impairs* The Recipient From**  
14 **Identifying The Sender Without Opening The Email**

15 Given that the Defendant put false information in the "From" field of the header, the only  
16 question that remains is whether Defendant's false information is "material," as that term is used  
17 and intended in the Act. If it is "material," then it violates the Act's prohibition against  
18 "materially" false or "materially" misleading header information.

19 Nowhere does the Act provide an exhaustive listing of what is meant by "materially false  
20 or materially misleading." Rather, when taken as a whole, the statutory language clearly  
21 indicates that Congress intends to leave the interpretation open to various unforeseen  
22 possibilities. The Act does provide several examples of things that would be considered  
23 "materially misleading" under section 7704(a)(1). Subsections (A) and (C) of 7704(a)(1)  
24

1 provide two such examples. The Plaintiff does not claim that either of these two subsections  
2 apply to the Defendants' spam, so they need not be considered further. At 15 USC  
3 7704(a)(1)(B) the Act takes the opposite approach, and provides a "safe harbor" by defining  
4 information not considered "materially misleading":

5  
6 (B) a 'from' line (the line identifying or purporting to identify a person initiating the  
7 message) that accurately identifies any person who initiated the message shall not be  
8 considered materially false or materially misleading;...

9 In this case, Defendant chose not to utilize this safe harbor. Had the Defendant chosen to  
10 "accurately identify the person who initiated" their spam, the emails would have complied with  
11 the Act. Instead, Defendant purposely chose not to do so. The only reasonable conclusion is  
12 that Defendant, widely known as a notorious spammer (and even sharing the name of a notorious  
13 computer virus), knows that if it accurately described itself as the sender in the "From name"  
14 portion of the header, a much larger percentage of their spam would get deleted without ever  
15 being opened.

16 Finally, 15 USC 7704(a)(6) provides that:

17  
18 (6) MATERIALLY- For purposes of paragraph (1), the term 'materially', when used with  
19 respect to false or misleading header information, includes the alteration or concealment  
20 of header information in a manner that would impair the ability of an Internet access  
21 service processing the message on behalf of a recipient, a person alleging a violation of  
22 this section, or a law enforcement agency to identify, locate, or respond to a person who  
23 initiated the electronic mail message or to investigate the alleged violation, or the ability  
24 of a recipient of the message to respond to a person who initiated the electronic message.

25 By its own terms, 15 USC 7704(a)(6) does not provide an exhaustive list of that which  
would be considered "materially" false or misleading. The word "includes" in the statute can

1 only be interpreted to mean that the scenarios set forth in 15 USC 7704(a)(6) are only some  
2 examples of “materially” false or misleading information, and that other possibilities exist.

3  
4 “The district court, in a carefully written and thoughtful opinion, construed “including” to  
5 mean, essentially, “such as.” Because this construction is consistent with the plain  
6 meaning of the language employed by Congress, the legislative history surrounding these  
7 provisions, and the reasonable interpretation given the language by the agency Congress  
8 directed to supervise the distribution of the funds at issue, we affirm. *Arizona State  
9 Board For Charter Schools v. U.S. Dept. of Edu.*, 464 F.3d 1003, 213 Ed. Law Rep. 114,  
10 06 Cal. Daily Op. Serv. 9047 (2006)

11 15 USC 7703 (d)(2), which sets forth the criminal offenses under the Act, contains a  
12 nearly identical definition of “materially,” except that the word “includes” is omitted.

13 Comparing the two sections, it becomes clear that Congress intended to have a wider variety of  
14 false and misleading information be considered as “material” in the standard set forth for civil  
15 violations set forth under 15 USC 7704(a)(6) than in the standard for criminal violations set forth  
16 under 15 USC 7703 (d)(2).

17 Even if the Act’s use of the word “includes” is ignored, and the more restrictive standard  
18 set forth in criminal section 7703 (d)(2) is “imported” to the civil section 7704(a)(6) and then  
19 applied, it is still clear that the Defendants violated that standard by substituting advertising copy  
20 for their name in the “from name” portion of their headers. Under this stricter standard, to be  
21 “materially false or misleading,” all that is required is “the alteration or concealment of header  
22 information in a manner that would impair the ability of ... a person ... to identify .. a person  
23 who initiated the electronic mail message.” 15 USC 7704(a)(6) (emphasis added). The Act  
24 doesn’t require the false information “prevent” the recipient from identifying the sender. All that  
25 is required is that the false information to “impair” that ability.

1 “Impair” is defined as “to cause to diminish, as in strength, value, or quality: *an injury*  
2 *that impaired my hearing; a severe storm impairing communications. The American Heritage®*  
3 *Dictionary of the English Language, Fourth Edition*, Houghton Mifflin Company, 2004. 06 Dec.  
4 2006. Replacing the actual, accurate name of the sender in the header with advertising copy  
5 meets this standard because it serves to “diminish” the “strength, value or quality” of the header  
6 information in identifying the person who initiated the electronic mail message. Given that the  
7 Defendants have deliberately, and admittedly hidden their true identity and replaced it with  
8 advertising copy, how could it not?  
9

10 The Federal Trade Commission (FTC), the entity charged by Congress with interpreting  
11 and enforcing the Act, has set forth the requirements of the “From” line in a manner entirely  
12 consistent with Gordon’s position. In the FTC’s guidance to commercial emailers, the FTC  
13 states that the “From” line “must be accurate and *identify the person who initiated the email.*”<sup>6</sup>  
14 (emphasis added)

15 The CAN-SPAM Act: Requirements for Commercial Emailers

16 What the Law Requires

17 It bans false or misleading header information. Your email's "From," "To," and routing  
18 information – including the originating domain name and email address – must be  
19 accurate and identify the person who initiated the email. (emphasis added).

20 The FTC’s interpretation of the Act is entirely consistent with the intention of the Congress, and  
21 requires that the header accurately identify the person who actually initiated the email.  
22

23 \_\_\_\_\_  
24 <sup>6</sup> <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>

**Omega World Travel v. Mummagraphics**

1  
2 No discussion of CAN-SPAM would be complete without recognizing the Fourth Circuit  
3 Federal Court of Appeals recent holding in Omega World Travel v. Mummagraphics, Inc. No.  
4 05-2080, 4<sup>th</sup> Cir., Nov. 17, 2006. In Omega, the Fourth Circuit held that the specific inaccuracies  
5 in the email header at issue in that case were not "materially false or materially misleading." The  
6 Omega decision never discloses what, if anything, the defendant "Cruise.com Inc." put in the  
7 "from name" portion of the email header. It is therefore impossible to discern from the opinion  
8 how the emails at issue would have actually appeared to a recipient in a typical email in-box.  
9 Furthermore, the domain name "cruise.com" used in the "from address" of the header discussed  
10 in Omega was identical to the actual corporate name of the defendant, "Cruise.com Inc." These  
11 facts readily distinguish Omega from the present case.  
12

13 Ignoring these factual distinctions, Gordon still argues that the Fourth Circuit's holding in  
14 Omega failed to apply black letter law of statutory construction, misconstrued the intent of  
15 Congress, and should not be followed by this or any other Court. Most troubling of all, the  
16 Omega Court determined whether information in the header was "materially false or materially  
17 misleading" by comparing it to information contained within the body of the spam email itself.  
18 The effect of this rule is to require the recipient of a spam email from a sender who has hidden  
19 their identity in the header to actually open that spam email to determine whether it violates the  
20 Act. The rule has the dual effect of eviscerating the Act's prohibition against false or misleading  
21 header information, and forcing spam email recipients to expose their computers to the risks  
22 discussed above, inherent in opening spam messages, thereby frustrating Congresses' intent.  
23  
24  
25

1 The Fourth Circuit also failed to adhere to the black letter law of statutory construction  
2 by erroneously interpreting 15 USC 7704(a)(6). Contrary to the Omega Court's holding, 15  
3 USC 7704(a)(6) does NOT limit the possible meanings of the term "materially" to those  
4 described in the section. As discussed above, a plain reading of 15 USC 7704(a)(6)  
5 demonstrates that Congress intended that section to merely provide non-exclusive examples of  
6 what constituted false and misleading header information. Accordingly, the Fourth Circuit erred  
7 when it construed 15 USC 7704(a)(6) as providing a strictly limited definition of the term  
8 "materially" in 15 USC 7704(a)(1).  
9

#### 10 **The Fourth Circuit's Preemption of Oklahoma's Anti-Spam Statute.**

11 The Fourth Circuit in Omega preempted the Oklahoma statute governing spam. The  
12 Washington CEMA statute at issue in this case is different from the Oklahoma statute, and  
13 therefore distinguishable on its facts. However, the Fourth Circuit's analysis of pre-emption is  
14 fatally flawed, and should not be followed.  
15

16 The Fourth Circuit correctly recognized that Congress created a national standard for  
17 commercial email with the CAN-SPAM Act. However, Congress plainly did NOT intend to  
18 have this standard apply in all areas governing commercial email. Congress explicitly stated:  
19

20 IN GENERAL- This Act supersedes any statute, regulation, or rule of a State or political  
21 subdivision of a State that expressly regulates the use of electronic mail to send commercial  
22 messages, except to the extent that any such statute, regulation, or rule prohibits falsity or  
deception in any portion of a commercial electronic mail message or information attached  
thereto. 15 USC 7707(b)(1) (emphasis added).  
23  
24  
25



1 The Omega Court simply ignored this language, and assumed that Congress intended that the  
2 national standard created by the Act would apply in all areas governing commercial email.  
3 However, it is clear that the Congress had no such intention. Rather, Congress specifically  
4 preserved the authority for the States to promulgate statutes, regulations, and/or rules prohibiting  
5 falsity or deception in any portion of a commercial electronic mail message or information  
6 attached thereto. The legislative history is clear on this issue.

7  
8 Thus, a State law requiring some or all commercial e-mail to carry specific types  
9 of labels, or to follow a certain format or contain specified content, would be  
10 preempted. By contrast, a state law prohibiting fraudulent or deceptive headers,  
11 subject lines, or content in commercial e-mail would not be preempted...

12 Given the inherently interstate nature of e-mail communications, the Committee  
13 believes that this bill's creation of one national standard is a proper exercise of the  
14 Congress's power to regulate interstate commerce that is essential to resolving  
15 significant harms from spam faced by American consumers, organizations, and  
16 businesses throughout the United States. This is particularly true because, in  
17 contrast to telephone numbers, e-mail addresses do not reveal the State where the  
18 holder is located. As a result, a sender of e-mail as a no easy way to determine  
19 with which State law to comply. Statutes that prohibit fraud and deception in the  
20 e-mail do not raise the same concern, because they target behavior that a  
21 legitimate business trying to comply with relevant laws would not be engaging in  
22 anyway. Sen. Rep. No. 108-102, at 21-22 (2003) (emphasis added).

23 There is really no question that Congress intended to allow the States wide latitude in  
24 governing falsity and deception, and had no intention whatsoever of applying a national standard  
25 over these consumer protection aspects of commercial email.

### **False or Misleading Headers That Violate CAN SPAM Also Violate CEMA**

26 Washington's Commercial Electronic Mail Act, RCW 19.190 et seq. (CEMA) is in most  
27 respects far more straightforward than the federal CAN SPAM Act. The specific provision that  
28 is relevant to show liability is RCW 19.190.020. It states:

1 (1) No person may initiate the transmission, conspire with another to initiate the  
2 transmission, or assist the transmission, of a commercial electronic mail message from a  
3 computer located in Washington or to an electronic mail address that the sender knows, or  
4 has reason to know, is held by a Washington resident that:

5 (a) Uses a third party's internet domain name without permission of the third party, or  
6 otherwise misrepresents or obscures any information in identifying the point of origin or the  
7 transmission path of a commercial electronic mail message; or

8 (b) Contains false or misleading information in the subject line.

9 (2) For purposes of this section, a person knows that the intended recipient of a  
10 commercial electronic mail message is a Washington resident if that information is available,  
11 upon request, from the registrant of the internet domain name contained in the recipient's  
12 electronic mail address.

13 All that Gordon need show is that 1) the emails sent by the Defendants "misrepresent or  
14 obscure any information in identifying the point of origin" and that 2) the "registrant of the  
15 internet domain name contained in the recipient's electronic mail address" will inform the  
16 Defendants that the recipient is a Washington resident. The Affidavits of individual email  
17 recipients who are users of the interactive computer service provided by Gordon submitted  
18 herewith establish the second requirement. All of the emails that form the basis of this Motion  
19 were sent to Gordon, or to one of the email addresses and internet domain names registered and  
20 owned by the forgoing affiants. All of these affiants have declared that, if asked, they would  
21 have identified themselves as the registrant of their domains, and as the owners of the email  
22 addresses as Washington residents. Further, all of these domain names and email addresses were  
23 operated on Gordon's server. All that remains to establish liability under CEMA is that Gordon  
24 must show the emails in question "misrepresent or obscure any information in identifying the  
25 point of origin." i.e., the "Sender".

1 Since the spam emails sent by Defendant violate Can-SPAM, they also violate CEMA. The  
2 information in the "From lines" of the Defendant's spam violates 15 USC 7704(a)(1) because it  
3 "contains, or is accompanied by, header information that is materially false or materially  
4 misleading." As such, it also violates CEMA because information in the "from lines" is  
5 supposed to identify the point of origin, and since the information in the "from lines" is  
6 "materially false or misleading" it also "misrepresents or obscures any information in identifying  
7 the point of origin." For the same reasons that the Court should rule that the spam emails sent by  
8 Defendant violates CAN SPAM, the Court should also rule that the spam emails sent by  
9 Defendant violates CEMA.  
10

### 11 Damages

12 15 USC 7706(g)(3)(A)(ii) provides for damages of "up to \$100, in the case of a violation  
13 of 5(a)(1)." Those damages may be tripled under 15 USC 7706(g)(3)(C)(i) "if the court  
14 determines that the defendant committed the violation willfully or knowingly." 15 USC  
15 7706(g)(4) provides that the court may require the payment of reasonable attorney fees. RCW  
16 19.190.040(2) provides that "(d)amages to an interactive computer service resulting from a  
17 violation of this chapter are one thousand dollars, or actual damages, whichever is greater."  
18 Defendant Virtumundo is one of the largest and most sophisticated email marketing companies  
19 in the world. Its conduct here was pervasive and intentional. If the words "willfully and  
20 knowingly" are to have any meaning whatsoever, they must, at a minimum, apply to this  
21 Defendant's conduct.  
22

23 For each spam email message sent to Gordon's ISP, Gordon is entitled to \$300 under  
24 CAN SPAM (\$100 tripled), plus \$1,000 under CEMA, ( $\$1,000 + \$300 = \$1,300$ ) or 8,082 times  
25

1 \$1,300 = \$10,506,600, plus attorney fees. Gordon therefore respectfully requests that the Court  
2 enter an Order awarding Gordon judgment in the amount of ten million five hundred six  
3 thousand six hundred dollars, plus reasonable attorney fees.

4  
5

6 **RESPECTFULLY SUBMITTED** this <sup>th</sup> 18 day of December, 2006.

7

8 DOUGLAS E. MCKINLEY, JR.  
Attorney at Law

MERKLE SIEGEL & FRIEDRICHSEN, P.C.

9

10 /S/ Douglas E. McKinley, Jr.  
Douglas E. McKinley, Jr., WSBA #20806  
Attorney for Plaintiffs

/S/ Robert J. Siegel  
Robert J. Siegel, WSBA #17312  
Attorney for Plaintiffs

11  
12

13  
14

15  
16

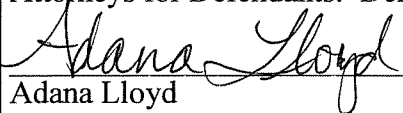
17  
18

19  
20

21 Certificate of Service

22 I, hereby, certify that on December 18, 2006, I filed this affidavit with this Court via approved  
23 electronic filing, and served the following:

Attorneys for Defendants: Derek A. Newman, Newman & Newman .

24   
Adana Lloyd

25