

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA, )  
 )  
Plaintiff, )  
 )  
v. )  
 )  
ROBERT ALAN SOLOWAY, and )  
NEWPORT INTERNET MARKETING, )  
 )  
Defendants. )  
\_\_\_\_\_ )

NO. CR07-187MJP

GOVERNMENT’S RESPONSE IN  
OPPOSITION TO MOTION  
TO DISMISS AGGRAVATED  
IDENTITY THEFT COUNTS

Noted: February 22, 2008

The United States of America, by and through Jeffrey C. Sullivan, United States Attorney for the Western District of Washington, and Kathryn A. Warma, Assistant United States Attorney for said District, files this Response in Opposition to the Defendant’s Motion to Dismiss Counts 19 - 25 of the Second Superseding Indictment.

**I. Introduction**

Defendant Robert Soloway (“Soloway”) argues in his Motion to Dismiss that the seven counts of Aggravated Identity Theft charged against him should be dismissed outright because: 1) the defendant’s conduct “was not aggravated in the sense that it was not the type of conduct for which the statute intended enhanced penalties to apply,” and 2) the identity theft conduct charged in counts 19-25 “is already covered” in Count 18 (alleging Fraud in Connection with Electronic Mail, in violation of 18 U.S.C. §1037(a)(3)). Motion to Dismiss, at pp. 4, 7. As will be demonstrated below, defendant’s assertions are meritless. The motion relying upon them should be denied.

1 **II. The Statute**

2 The “Aggravated Identity Theft” statute provides, in pertinent part:

3 **§ 1028A. Aggravated identity theft**

4 **(a) Offenses.-**

5 **(1) In general.-** Whoever, during and in relation to any felony violation  
6 enumerated in subsection (c), knowingly transfers, possesses, or uses, without  
7 lawful authority, a means of identification of another person shall, in addition to  
8 the punishment provided for such felony, be sentenced to a term of  
9 imprisonment of 2 years.

10 **(c) Definition.-** For purposes of this section, the term “felony violation  
11 enumerated in subsection (c)” means any offense that is a felony violation of -

12 (4) any provision contained in this chapter (relating to fraud and  
13 false statements), other than this section or section 1028(a)(7);

14 (5) any provision contained in chapter 63 (relating to mail, bank,  
15 and wire fraud). . .

16 The statute thus clearly provides that a perpetrator of any number of federal  
17 felonies - specifically including §1037, (“fraud in connection with electronic mail,”<sup>1</sup>) as  
18 well as mail and wire fraud - is criminally responsible for the additional crime of  
19 aggravated identity theft if, “during and in relation to” those other crimes, he or she  
20 also “knowingly transfers, possesses, or uses, without lawful authority, a means of  
21 identification of another person.”

22 The term “means of identification” is in turn defined for purposes of 18 U.S.C.  
23 §1028A, in 18 U.S.C. §1028(d)(7) as, “any name or number that may be used, alone  
24 or in conjunction with any other information, to identify a specific individual . . .”

25 The statute goes on to identify, by way of example and not of limitation, an expansive  
26 list of possible identifiers that includes, *inter alia*: name, “unique electronic  
27 identification number, address, or routing code,” and “telecommunication identifying  
28 information.”

29 **III. Argument**

30 **A. Soloway Knowingly, Willfully, and Repeatedly Engaged in Egregious  
31 Acts of Identity Theft that Fall Squarely within the Terms of the Aggravated  
32 Identity Theft Statute**

33 \_\_\_\_\_  
34 <sup>1</sup>Section 1037 is contained in the “chapter” (Chapter 47, Title 18, United States Code) referenced in subsection  
35 (c)(4).

1 From November 2003, until his arrest in May of 2007,<sup>2</sup> Robert Soloway devised  
2 and executed a multi-faceted criminal scheme that generated over a \$1,000,000 in  
3 proceeds. The scheme can be summarized as follows:

4 Soloway created and published a series of Internet websites on which he touted  
5 his “low cost,” but purported high return “distribution email” advertising product and  
6 service; *i. e.*, Soloway was offering to sell a software product that would enable the  
7 customer to send out their own high volume e-mail ads, or to send out “distribution  
8 email” ads on behalf of the customer. Soloway, however, made numerous material  
9 false and fraudulent representations on these various websites - most notably including  
10 the purported “opt-in” character of the e-mail addresses used in the “distribution  
11 email” product and service, but also regarding the availability of customer support and  
12 payment of “full 100%” refunds, “no questions asked,” to product customers.<sup>3</sup>

13 Soloway promoted and advertised his websites - and thus his scheme - by  
14 indiscriminately blasting the Internet and e-mail users world-wide with hundreds of  
15 millions - likely even billions - of “spammed” e-mail commercial messages. These  
16 spammed messages were transmitted in violation of two separate subsections of the  
17 “CANSPAM Act,” as codified at 18 U.S.C. §1037, because Soloway routinely used  
18 “proxy” computers to relay his spam, (§1037(a)(2)), and also routinely materially  
19 falsified header information (§1037(a)(3)). As the Court will hear at trial, these two  
20 techniques are common “spammer” tools which, if used in combination, effectively  
21 mask the two primary and most obvious means of identifying the source of a spammed  
22 e-mail message.<sup>4</sup>

---

23  
24 <sup>2</sup>Evidence exists to show that Soloway had run the same scheme, likely for years, in California and Oregon before  
moving to Washington in 2003.

25 <sup>3</sup>Because Soloway executed his scheme to defraud by way of interstate wire communications (in publishing the  
26 websites) and by sending materials (the “product” he promoted and sold) through the mails and commercial interstate  
carriers, he has been charged with both wire and mail fraud (Counts 1-16, Second Superseding Indictment).

27 <sup>4</sup>The use of “proxy” relays to transmit e-mail conceals the identifying Internet Protocol (“IP”) address of the true  
28 originating computer, and the falsification of the “from” field in headers conceals the text-based name of the message  
“sender”.

1 Soloway went beyond these “basic” spammer ruses, however, by choosing to  
2 engage in substantially more aggressive tactics involving the theft and unauthorized use  
3 of e-mail addresses and domain names that had been purchased and were owned by  
4 actual people, who were individually identifiable therefrom. As explained more fully  
5 below, and as will be proved at trial, these individuals suffered harm financially, as  
6 well as to their names and reputations, as a direct result of Soloway’s knowing,  
7 intentional, and repeated theft of their identities in furtherance of his mail and wire  
8 fraud scheme, and in relation to his felony “CANSPAM” Act violations.

### 9 “Spamming 101”

10 In order to best understand the significance of Soloway’s identity theft crimes, it  
11 is useful first to review some spamming “basics.”<sup>5</sup>

12 Unlike telemarketers or junk mailers, spammers can almost instantaneously<sup>6</sup>  
13 “blast” their commercial advertisements at a barely perceptible financial cost to  
14 virtually hundreds of millions of recipients, world-wide. Also, unlike telemarketers or  
15 junk mailers, the costs of doing so do not measurably increase with an increase in the  
16 volume of the target audience. Consequently, spammers routinely seek to maximize  
17 their “mailing lists,” based on the assumption that the chances of a financial return  
18 (often from the “sale” of something fraudulent) will increase proportionately with the  
19 size of the receiving audience. The spammers themselves typically incur no additional  
20 costs for spamming ever more addresses - even if many of the e-mail addresses are  
21 bogus or invalid and therefore “bounce back” when they can not be delivered as  
22 addressed. Creating ever larger e-mail address lists (either for their own use or for  
23 sale,) is therefore a constant goal of spammers.

---

24  
25 <sup>5</sup>The government will present an expert witness at trial who will provide testimony on these and other aspects of  
26 “spam,” including what it is, how it’s distributed, how spammers profit, and the damages it causes and financial costs it  
27 creates for everyone who uses the Internet, but particularly for small Internet businesses and Internet Service Providers  
28 (“ISPs”). See also: Fighting Spam for Dummies, J. Levine, M. Levine Young, and R. Everett-Church, Wiley Publishing,  
2004; and Canning Spam, J. Poteet, Sams Publishing, 2004.

<sup>6</sup>Indeed, the speed and immediacy of spam has made it a favored technique for natural disaster and “catastrophe”  
fraud.

1 One method of creating and “bulking up” e-mail address lists is through  
2 “dictionary attacks.” This typically involves the use of a computer program to generate  
3 long lists of possible names that are then appended to a known - or even a similarly  
4 generated - domain name. For example, a series of generated names (Alice, Ann,  
5 Amy), could be attached with the “@” symbol to the domain name: “usdoj.gov.”  
6 Spammed messages could then be blasted to every one of those computer generated e-  
7 mail addresses in the hope that one or more would by chance be valid. An example of  
8 a “dictionary attack” list is appended as Attachment A.<sup>7</sup>

9 Another method of obtaining e-mail addresses and domain names is through  
10 “address harvesting.” Address harvesting has also become “automated” with the use of  
11 computer programs designed to “crawl” the Internet, visit websites and databases that  
12 might contain e-mail addresses or domain names, and compile those for the  
13 “harvester.” Address harvesting has the advantage of yielding lists of addresses and  
14 domain names that may well be valid, insofar as they were surreptitiously stolen,  
15 without permission, from active website or databases. The existence of these harvested  
16 addresses or domain names does not, however, in any way signify permission by the  
17 owners of the same to be included on spam address lists for which they have never, in  
18 any sense, “opted in.” Evidence will be presented at trial to prove that Soloway was  
19 using “harvested addresses,” in addition to “dictionary attacks” for his illegal spam.

20 Regardless of whether a spammer gets address lists from dictionary attacks,  
21 address harvesting, or (as in Soloway’s case), from a combination of both, the  
22 addresses on those lists need only be inserted (again, via an automated program) into  
23 the “to” field in a spam “header” in order to blast the spam messages off, in bulk, to  
24 those separate addresses. In order to conceal his/her identity as the “sender,” the  
25 spammer can then manipulate or forge the “from” field in the header either to contain a

---

26  
27 <sup>7</sup> This particular list was contained on one of the “product” CDs that was advertised and sold by Soloway from  
28 his website. Although Soloway represented (fraudulently) that the product he sold contained valid and “opt-in” e-mail  
addresses, the (defense contracting company) that owns the domain name, “amiinter.com” has confirmed that these 400 e-  
mail addresses built on the domain name “amiinter.com” are neither valid nor “opt-in.”

1 false, fabricated, or non-existent name, or even to be blank. Spammers can, and most  
2 often also “rotate” a variety of false and fabricated names in the “from” header, as they  
3 continue to blast out repeated multiple versions of the same spam message - again, in  
4 an attempt to maximize the number of spam messages they send and hope will be  
5 received, without regard to the desires of, or impact on the target audience.

### 6 **Anti-Spam Measures**

7 Spam is universally regarded within the Internet community as a costly, invasive  
8 and deleterious “scourge.” It is commonly estimated that spam usurps 80% or more of  
9 Internet “bandwidth,” and costs Internet users billions of dollars annually. Some of  
10 those costs are spread among the universe of all Internet users; others are suffered in  
11 particular by ISPs and by small Internet-based businesses. Spam is also recognized as  
12 the “delivery mechanism” for pernicious fraud and “phishing” schemes, pornography,  
13 and a host of “malware” that includes viruses, worms, trojans, and spyware.

14 The economic and societal costs of spam have driven law-making bodies world-wide to  
15 enact both civil and criminal “anti-spam” statutes. Reputable ISPs have uniformly  
16 adopted rigorous anti-spam policies that are incorporated into their terms of service.  
17 Subscribers who are identified to have violated an ISP’s anti-spam policies can and  
18 often have their accounts terminated, thereby ending their ability either to send or  
19 receive e-mail from that address. Anti-spam products and services have also been  
20 developed and made commercially available. These include a variety of “spam  
21 filtering” products and services, as well as “spam blacklists.”

22 Simply stated, spam filtering is designed to keep spam out of systems, networks  
23 and “in-boxes.” Filtering can be done with a variety of technical approaches and  
24 systems, and with a varying range of efficacy, and cost. None among these products or  
25 services is “perfect,” however. No filtering can stop all spam, and some can even  
26 result in “false positives,” which means that legitimate e-mails, too, will be blocked.

27 Spam “blacklists” are developed by a variety of online organizations (some non-  
28 profit, some commercial), based on data compiled from Internet traffic that is identified

1 as spam or spam-related. The blacklists are then used in conjunction with filtering  
2 products and services to exclude spam with those identifiers, and by ISPs to terminate  
3 accounts identified on the blacklists or to block incoming traffic from those accounts.

4 **Soloway’s Knowing, Willful, and Repeated Acts of Identity Theft in**  
5 **Furtherance of Wire Fraud and CANSPAM Act Violations**

6 Evidence at trial will establish that Soloway was keenly aware of anti-spam  
7 measures including filtering, and ISP anti-spam policies. Indeed, his repeated,  
8 knowing and willful use of legitimate e-mail addresses and domain names, including  
9 those paid for and belonging to identifiable individuals, without their permission and  
10 against their expressed will, was a tactic that he intentionally embraced and exploited,  
11 in the words of his own counsel, precisely “to circumvent . . . spam filter[s].”<sup>8</sup> This  
12 particular tactic enables the spam sender to thwart spam filters because the e-mail  
13 recipient can not filter based on his/her own e-mail address - as to do so would  
14 effectively preclude any e-mail addressed to the recipient, from being received by the  
15 recipient.<sup>9</sup> It is thus a means to force the owner of any given e-mail address either to  
16 continue receiving the spam, in perpetuity and in whatever volume it arrives - or to  
17 surrender that e-mail address or domain name. Surrendering an established e-mail  
18 address or domain name can be financially devastating to a small business that has built  
19 its reputation on it from its inception.

20 Soloway thus proved himself a savy and aggressive spammer who deliberately  
21 tailored his spamming techniques to defeat protections put in place to defeat spamming,  
22 and who was absolutely indifferent to the consequences of his actions to his innocent  
23 victims. Soloway also was aware - but resolutely indifferent to - the fact that many of  
24 these victims often suffered yet again - when they were blacklisted as a result of his  
25 spamming activity because their legitimate and individually identifiable e-mail

---

26 <sup>8</sup>Motion to Dismiss, at p. 2, line 18.

27 <sup>9</sup>Some advanced filtering products or services can possibly defeat this tactic by relying on “scores” or factors  
28 independent of the “from” information. These products or services, however, are not necessarily available - or within the  
financial or technological reach - of all Internet users.

1 addresses and domain names had been identified with spam that he - not them - had  
2 sent, and was responsible for.

3 All of the aggravated identity theft counts charged in this case involve victims  
4 whose experiences with Soloway shared common traits.<sup>10</sup> Most of the individuals  
5 (identified by their initials for purposes of the Indictment) began receiving spammed e-  
6 mail messages, sometime during the period from 2005 until 2007, that contained  
7 advertisements for, and a link to Soloway's (fraudulent) websites. As is typically the  
8 case with spam, these spammed messages came over, and over. And to the horror of  
9 each of these individuals, the messages included a header that identified the recipients  
10 themselves as the "sender" of spam that advertised a company they had never heard of  
11 and had nothing to do with. None of the recipients had "opted-in" to receive any such  
12 spammed advertisements, and none wished to be associated in any way with a company  
13 responsible for spam. Most of these individuals contacted Soloway repeatedly, and  
14 requested that he stop using their e-mail addresses and domain names in spam.  
15 Soloway ignored these requests, and continued to spam, using the e-mail addresses and  
16 domain names owned by these victim individuals, despite their voiced objections. In  
17 some cases the spam even increased. Several of these victims will testify further that  
18 they received either "bounce backs" to their addresses, indicating that Soloway had  
19 forged their addresses into the "from" header into spam he had sent to third parties, or  
20 complaints directly from third parties who blamed them for spam. And finally, several  
21 of these victims will testify that they subsequently were blacklisted by one or more ISPs  
22 or filtering services, because the e-mail address or domain name they owned - and that  
23 had been used by Soloway without their authority - had become identified as having an  
24 association with spam. Their individual reputations, and those of their businesses were  
25 compromised; they lost customers and the ability to do business on-line.

---

26  
27  
28 <sup>10</sup>The victims associated with counts 19 - 26 are but a representative sample of many more who were identified during the investigation as suffering like experiences.

1 By way of illustration, additional details regarding two of these individual victims are  
2 as follows:

3 Count 19: R.M. will testify that he had registered and purchased a domain name  
4 that consisted of his combined first and last name, followed by “.net”. Beginning in  
5 March of 2005, his wife (with a different name and who used an entirely different e-  
6 mail account,) began receiving spammed advertisements from several different  
7 companies. R.M.’s wife had not opted-in to receive any such spammed advertisements.  
8 The header of these spams identified the “sender” with one of a variation of names “at”  
9 the domain name owned and registered to R.M. R.M. had no association with any of  
10 these companies, nor had he authorized any one to use his personal, individually  
11 identifiable name for spamming. R.M. contacted two of these companies, and was told  
12 they had each hired Soloway, relying on his representations that he would send  
13 “broadcast emails” to “opt-in” e-mail lists on their behalf. Both companies complained  
14 that Soloway had defrauded them, and was instead spamming advertisements for their  
15 company to recipients who were not opt-in, and from whom they had received  
16 complaints. R.M. did some investigatory work of his own, and located a phone  
17 number for Soloway. He called the number to complain about the unauthorized use of  
18 his individually identifiable domain name - a domain name he had purchased and  
19 registered. The person answering the telephone hung up on him. R.M. called again  
20 and asked to speak to the owner or manager. The person answering the phone hung up  
21 on him again.<sup>11</sup> Spam with R.M.’s individually identifiable domain name continued,  
22 causing R.M. to file a complaint with the FBI.

23 Count 20: T.C. will testify that in September, 2005, he began receiving spam at  
24 several domain names and e-mail addresses that he owned, including an “individually  
25 identifiable” e-mail address that consisted of his first and last name, at

---

27 <sup>11</sup>Numerous victims have reported that Soloway - who was the sole owner/operator and employee of his company  
28 - routinely hung up if they telephoned to object or complain. Soloway would stay on the phone if the customer was placing  
an order for service or product.

1 ["universalbyte.com"](http://universalbyte.com). The spam advertised, and contained links to Soloway's  
2 websites. T.C. had never opted in to receive this spam, and was distressed to see that  
3 the headers were forged in a way to make it appear as though the spam had been sent  
4 by him, from his own e-mail addresses and domain names. T.C. received up to 200  
5 such spams daily. T.C. also received "bounce backs" to his addresses and domain  
6 names, indicating to him that spam with his addresses forged into "from" header fields  
7 had been transmitted to others. T.C. used the "unsubscribe" tool on Soloway's  
8 website, and also sent e-mail to the administrative contact identified in a WHOIS  
9 lookup of Soloway's website to demand that the spam using his addresses be stopped.  
10 The spam from Soloway with T.C.'s individually identifiable e-mail address forged into  
11 header "from" fields continued. T.C. was forced to close his main e-mail address,  
12 which had been his primary work e-mail address. Domains owned by T.C., the names  
13 of which Soloway had forged into "from" headers in spam, were also blacklisted by  
14 AOL and Hotmail, forcing him to give up ownership of those domain names, as well.

15 The e-mail addresses and domain names of R.M, T.C., and all of the other  
16 victims named in the aggravated identity theft counts either consist of, or contain their  
17 own individual names, or consist of a company name that is unique and either "alone,  
18 or in conjunction with . . . other information," identifies a specific individual. They  
19 are thus "means of identification," as that term is defined for purposes of 18 U.S.C.  
20 §1028A. They were "knowingly transferred, possessed or used" by Soloway, "without  
21 lawful authority" - forged by Soloway in the headers of spammed messages that were  
22 intended to further his wire/mail fraud scheme, and that were sent in violation of two  
23 separate provisions of 18 U.S.C. §1037. The victims themselves contacted Soloway to  
24 object and to direct him to stop the identity theft, thereby confirming the fact (and his  
25  
26  
27  
28

1 knowledge) that the identities he had stolen belonged to “actual people” who did, in  
2 fact, object to their theft and unauthorized use.<sup>12</sup>

3 Soloway’s knowing, intentional and repeated egregious acts of identity theft fall  
4 squarely within the terms of the Aggravated Identity Theft statute. To the extent that  
5 any factual disputes over these violations exist, they properly should be resolved by the  
6 jury at trial. United States v. Beachem, *supra*, at 1158.

7 **B. The Egregious Acts of Identity Theft Committed Repeatedly by Soloway**  
8 **and NIM Constitute Offenses Separate and Distinct From What is Needed to**  
9 **Charge Violations of 18 U.S.C. § 1037(a)(3)**

10 While not characterized as such, defendant’s argument that the aggravated  
11 identity counts are “covered” by the §1037(a)(3) count is essentially one that these  
12 counts are multiplicitous. An indictment is multiplicitous if “it charges multiple counts  
13 for a single offense, producing two penalties for one crime and thus raising double  
14 jeopardy questions.” United States v. Stewart, 420 F.3d 1007, 1012 (9th Cir. 2005).

15 Counts within an indictment are not, however, multiplicitous if “each separately  
16 violated statutory provision requires proof of an additional fact which the other does  
17 not.” *Id.*

18 [T]he test to be applied to determine whether there are two offenses  
19 or only one, is whether each provision requires proof of a fact which the  
20 other does not . . . A single act may be an offense against two statutes;  
21 and if each statute requires proof of an additional fact which the other  
22 does not, an acquittal or conviction under either statute does not exempt  
23 the defendant from prosecution and punishment under the other.

24 Blockburger v. United States, 284 U.S. 299, 404 (1932). “Congress has the power to  
25 establish that a single act constitutes more than one offense, at least as long as each  
26 offense requires proof of a fact the other does not.” United States v. Stearns, 550 F.2d  
27 1167, 1172 (9th Cir. 1977); *See also*: United States v. Rude, 88 F.3d 1538 (9th Cir.

---

28 <sup>12</sup>As noted by the Defense in their Motion to Dismiss, there is a split among courts as to the *mens rea* requirement of 18 U.S.C. §1028A, with this Court holding in United States v. Beachem, 399 F. Supp. 2d 1156, 1158 (U.S.D.C. W.D. WA. 2005) that “knowingly,” as used in §1028A applies to “another person.” That standard is met in this case, because Soloway was repeatedly notified by the identity theft victims themselves that he was using their identities without their authority, and must stop doing so. Soloway brazenly continued to use their stolen individually identifiable e-mail addresses and domain names even after these objections were made.

1 1996), (indictment using same wire transfers as basis for wire fraud and money  
2 laundering is not multiplicitous).

3 The crimes defined in sections 1028A(a)(1) and 1037(a)(3) of Title 18 are  
4 distinct offenses, requiring proof of different facts for conviction. Conviction under  
5 §1037(a)(3) requires proof that: 1) in, or affecting interstate commerce, 2) the  
6 defendant materially falsified header information, 3) in “multiple” commercial e-mail  
7 messages, and 4) that defendant intentionally initiated the transmission of those  
8 messages. Conviction under §1028A(a)(1) requires proof that: 1) during or in relation  
9 to one of the enumerated felonies, 2) the defendant knowingly transferred, possessed or  
10 used, without lawful authority, 3) a means of identification of another person.

11 Proof of one of these offenses does not satisfy proof of the elements of the other.  
12 They are not multiplicitous.

#### 13 **IV. Conclusion**

14 Whereas a prosecutor “plays a strictly advisory role in sentencing decisions. . .  
15 [he or she] retains almost absolute discretion in charging decisions.” In re Morgan,  
16 506 F.3d 705, 711 (9th Cir. 2007). “In our system, so long as the prosecutor has  
17 probable cause to believe that the accused committed an offense defined by statute, the  
18 decision whether or not to prosecute, and what charge to file . . . generally rests  
19 entirely in his discretion.” Bordenkircher v. Hayes, 434 U.S. 357 (1978).

20 Evidence well beyond the probable cause - even beyond the reasonable doubt -  
21 level, exists to support the §1037(a)(3), as well as the separate and distinct  
22 §1028A(a)(1) charges in this case. Defendant’s Motion to Dismiss Counts 19 - 25  
23 should be denied.

24 DATED this 14th day of February, 2008.

Respectfully submitted,  
JEFFREY C. SULLIVAN  
United States Attorney

25  
26 /s/ Kathryn A. Warma  
Assistant U.S. Attorney  
27 Email: [Kathryn.Warma@usdoj.gov](mailto:Kathryn.Warma@usdoj.gov)  
28 (206) 553-8786; Fax (206) 553-2502

CERTIFICATE OF SERVICE

I hereby certify that on February 14, 2008, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s). I hereby certify that I have served the attorney(s) of record for the defendant(s) that are non CM/ECF participants via telefax.

/s/ Lissette Duran-Leutz  
Lissette Duran-Leutz  
Legal Assistant  
United States Attorney's Office  
Western District of Washington  
700 Stewart Street, Suite 5220  
Seattle, Washington 98101-1271  
Tel.: (206) 553-7234  
Fax: (206) 553-2502  
E-mail: Lissette.I.Duran-Leutz@usdoj.gov