

1 **II. The Sentencing Hearing**

2 Soloway pleaded guilty to single counts of the crimes of mail fraud, fraud in electronic
3 mail (“criminal spamming”), and willful failure to file a tax return on March 14, 2008 - 10 days
4 before his scheduled trial on multiple counts of those crimes, as well as multiple counts of wire
5 fraud, aggravated identity theft, and money laundering. While his plea foreclosed a trial, all other
6 sentencing issues were reserved for the sentencing hearing. Because the government bears the
7 burden of proof on those issues, and because this case involves specialized technological
8 information in relation to newly emerging law, the government requested two days of sentencing
9 hearing time in order to present a complete and comprehensible picture of the nature and
10 circumstances of Soloway’s crimes as they pertain to all sentencing, and also forfeiture issues.

11 The government will present witnesses and evidence at the hearing, to include the
12 following: FBI Special Agent Ken Schmutz and FBI computer analyst Tom Ervin will present
13 evidence regarding Soloway’s criminal spamming operation - how he used a succession of e-mail
14 servers and proxies to transmit and relay the spam in a way that disguised the originating source -
15 both the Internet Protocol (“IP”) address, and through forged “header” information. By way of
16 these (criminal) techniques, Soloway was able to persist with his criminal spamming for years,
17 evading the types of detection techniques which will often defeat spamming. These witnesses,
18 and Steven Collins, who provides network security for a server company whose servers were
19 rented fraudulently by Soloway for spam transmission - will present evidence, as well, of the
20 volume of spam attributable directly to Soloway (direct evidence of hundreds of millions of
21 spammed messages, within even very limited periods of time). Adam Sweaney, who is himself
22 pending sentencing on federal charges related to botnet activity, will testify that Soloway rented a
23 botnet - a network of hacked computers - from him presumably to facilitate his “bulking”
24 (spamming) activities.

25 Spam expert John Levine, Ph.D., will provide further instructive technical information
26 regarding spamming techniques and tactics, including “address harvesting,” “dictionary attacks,”
27 and header forging - all of which were used by Soloway to advance his criminal spamming
28

1 scheme. Dr. Levine, and also Brian Sullivan, Vice President of Communication Services
2 Operations for AOL, will testify about the costs of criminal spam to the Internet infrastructure,
3 and to every user of it. Mr. Sullivan will also speak to the particular costs and damages suffered
4 by major Internet Service Providers (“ISP’s”), as well as the array of tools they must necessarily
5 deploy to protect their products and customers from the blight of criminal spam.

6 Testimony from all the self-identified victims in this case would take weeks. The
7 government will therefore present a handful of victims who are representative of the various
8 categories of victims harmed by Soloway’s criminal spamming and fraud scheme. These include
9 “customers” (Alice Hoffman, Christopher Leeds) who were defrauded through the purchase of
10 his “distribution e-mail” (spamming) “product” and “service.” Rev. Thom Miller, who believed
11 that Soloway would provide his non-profit ministry with “free” “broadcast e-mail service,” will
12 testify about the losses he likewise sustained when his charity’s website was shutdown for
13 “spamming” thereafter.

14 Innocent Internet users who were never customers of Soloway, but who were victimized
15 and suffered real and significant financial losses from Soloway’s criminal spamming, will also
16 explain these experiences and their consequent financial losses. These victims include Toby
17 Corbalis, a businessman from England; David Reel, owner of a small business in Florida; Robert
18 Braver, who ran a small ISP in Oklahoma; and Jason Nast, network security for the Santa
19 Barbara, CA, Social Services Department.

20 Finally, IRS Special Agent Silvia Reyes will present evidence regarding the proceeds of
21 Soloway’s criminal activities, all of which are forfeitable to the United States pursuant to the
22 CAN-SPAM Act. This evidence is relevant, as well, to “loss” for sentencing purposes.

23 **III. Relevant Facts**

24 Soloway moved to Seattle around November of 2003,¹ and from that time until his arrest
25 on May 30, 2007, continuously operated a criminal spamming and fraud scheme from the secure
26 comfort of his luxury apartment in downtown Seattle.

27
28 ¹Exhibit A, Harbor Steps Lease Agreement, 11/28/03.

1 Soloway had actually begun his “broadcast e-mail” business years earlier, in California,
2 and was operating it under the name of Newport Internet Marketing by 1997. The essential
3 “business model” used by Soloway then, and until the day of his arrest, was this: he would
4 transmit large volumes of unsolicited commercial e-mail messages (“spam”) to unknown
5 recipients. The spammed messages advertised Soloway’s own “distribution e-mail” (spamming)
6 business, and contained a “link” that could be “clicked” to connect to his commercial websites.
7 The websites contained more content advertising his commercial “distribution e-mail”
8 (spamming) business, as well as the means to order his “product” (software that would
9 purportedly enable the purchaser to send his own “broadcast e-mail”). (Later, Soloway also
10 advertised and sold a “distribution e-mail” [spamming] service.)

11 By 1999, California had passed one of the country’s first criminal spam statutes, and by
12 July of that year the Healdsburg CA Police Department had opened a criminal investigation of
13 Soloway based on complaints of violations of the California law.² While the complainant in that
14 case was a resident of Healdsburg, the investigating officer learned that complaints about
15 Soloway’s spamming had been made by people and companies worldwide, (including the
16 Japanese government, and several State Attorneys General), and that between them, the victims
17 had made claims for losses totaling over \$500,000.00. He learned, as well, that another case had
18 been opened on Soloway by the Cotati Police Department, and that another California spamming
19 victim had sent a registered cease and desist order to Soloway banning him from sending spam
20 through his servers.³ Although the investigating officer recommended that criminal charges be
21 filed against Soloway based on violations of the California criminal spam statute, they were not.
22 The officer did note that during his interview, Soloway “apologized for his e-mail practices, said
23 he has learned a lot.”⁴ Meanwhile, Soloway relocated himself and his business to the State of
24 Oregon.

25
26 ²Exhibit B, Healdsburg CA Police Dept. Incident Report, No. 99-1845.

27 ³*Supra*, at page 8.

28 ⁴*Supra*, at page 12.

1 Soloway then continued his spamming business from several locations in Oregon,
2 engendering complaints there, too, about his spamming activity.⁵ Though his profits were high
3 (allowing him to purchase a home and several expensive automobiles), Soloway soon again
4 relocated to Washington, late in 2003. And as professional “bulker” Soloway was most certainly
5 aware, it was at this same time that Congress approved, the President signed, and the first federal
6 anti-spamming law took effect on January 1, 2004.

7 **The CAN-SPAM Act of 2003**

8 By 2003, Congress recognized that the problems created and burdens imposed on
9 interstate commerce by spam necessitated legislative action. It responded with the CAN-SPAM
10 Act of 2003, imposing limitations and penalties - both civil and criminal - “on the transmission
11 of unsolicited commercial electronic mail (‘e-mail’) via the Internet.”⁶ In so doing, Congress
12 emphasized the extreme importance of e-mail communication to the public, their reliance on it
13 both for personal and commercial purposes, and its importance to the growth of commerce.
14 Congress also found:

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

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

20 (4) The receipt of a large number of unwanted messages also decreases the
21 convenience of e-mail and creates a risk that wanted e-mail messages, both

22 ⁵Exhibit C, Complaints filed with Better Business Bureau in 2003, while Soloway was still a
23 resident of Oregon.

24 For purposes of this Sentencing Memorandum, the government has identified and appended
25 records of complaints filed about Soloway with the Better Business Bureau, which records were
26 compiled and maintained in the regular course of business, and provided to the government with a
27 certification consistent with Rule 11, Federal Rules of Evidence, for business records. It is important to
28 note, however, that complaints about Soloway, numbering in the hundreds, have been filed with a
multitude of agencies, including the FTC, IC3, and WA and OR Attorneys General. Examples of
complaints filed with these other agencies are attached as Exhibit D.

27 ⁶“Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,” Pub. L.
28 108-187, codified at 15 U.S.C. §7701, *et seq.*, and 18 U.S.C. §1037.

1 commercial and noncommercial, will be lost, overlooked, or discarded amidst the
2 larger volume of unwanted messages, thus reducing the reliability and usefulness
of e-mail . . .

3 (6) The growth in unsolicited commercial e-mail imposes significant
4 monetary costs on providers of Internet access services, businesses, and education
and nonprofit institutions that carry and receive such mail, as there is a finite
5 volume of mail that [they] can handle without further investment in infrastructure.

6 (7) Many senders of unsolicited commercial e-mail purposefully disguise
7 the source of such mail.

8 (9) While some senders of commercial e-mail . . . provide simple and
9 reliable ways for recipients to reject (or “opt-out” of) . . . [future messages], other
10 senders . . . refuse to honor the requests of recipients not to receive e-mail from
such senders in the future . . .

11 (10) Many senders of bulk unsolicited commercial e-mail use computer
12 programs to gather large numbers of e-mail addresses on an automated basis from
13 Internet websites or online services where users must post their addresses in order
14 to make full use of the website or service.⁷

15 As protections for e-mail users, Congress therefore mandated requirements for the
16 transmission of commercial e-mail, explicitly including prohibitions on false or misleading
17 “headers”; the required inclusion of valid and functioning “return” e-mail addresses; and
18 prohibitions on continued transmissions after a recipient has elected to “opt-out,” as well as the
19 sale, or transfer of an “opted out” e-mail address to another.⁸

20 Congress provided for civil enforcement of the law by specified federal agencies,
21 including the Federal Trade Commission; by State Attorneys General; and by providers of
22 Internet services (“ISPs”).⁹ Civil damages were authorized, of \$25.00 to \$100.00 per violation of
23 the Act, as were “aggravated” damage awards¹⁰ if the defendant committed the violations
24 willfully or knowingly, or with other aggravating factors including “address harvesting” (e-mail
25 address of the recipient “was obtained using an automated means from an Internet website or
26 proprietary online service operated by another person . . .”) or “dictionary attacks” (e-mail
27
28

⁷Pub. L. 108-187, Section 2, (emphasis added).

⁸*Supra*, at Section 5.

⁹*Supra*, at Section 7.

¹⁰*Supra*, at Section 7(f)(3).

1 address of the recipient “was obtained using an automated means that generates possible e-mail
2 addresses by combining names, letters, or numbers into numerous permutations.”¹¹

3 Congress also adopted criminal spamming provisions at Section 4 of the Act,
4 “Prohibition Against Predatory and Abusive Commercial E-Mail,” through adoption of Section
5 1037 of Title 18, United States Code, “Fraud and related activity in connection with electronic
6 mail.” This statute criminalizes specified fraudulent e-mail practices in interstate or foreign
7 commerce that include transmitting bulk commercial e-mail (“spam”) through the computers of
8 others without authorization, using computers on the Internet to relay or retransmit spam with the
9 intent to deceive recipients or ISPs as to the origin of the messages, materially falsifying header
10 information, and materially falsifying domain name registrations. §1037(a). Penalties include
11 imprisonment for up to five years if the offense is in furtherance of another felony.
12 §1037(b)(1)(A).

13 Congress specified that “loss” for purposes of the criminal spamming statute was to have
14 the same expansive definition contained in 18 U.S.C. §1030 (“any reasonable cost to any victim,
15 including the cost of responding to an offense, conducting a damage assessment, and restoring
16 the data, program, system, or information to its condition prior to the offense, and any revenue
17 lost, cost incurred, or other consequential damages incurred because of interruption of service”),
18 and also that a Court, in sentencing a person convicted of a §1037 violation, “shall order that the
19 defendant forfeit to the United States - (A) any property, real or personal, constituting or
20 traceable to gross proceeds obtained from such offense,” and any equipment used to commit the
21 crime. §1037(d) and (c), (emphasis added).

22 Finally, Congress pronounced that “[s]pam has become the method of choice for those
23 who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and
24 Trojan horses into personal and business computer systems;” and directed the Department of
25 Justice to “use all existing law enforcement tools to investigate and prosecute those who send
26

27 ¹¹*Supra*, at Section 5(b).
28

1 bulk commercial e-mail to facilitate the commission of Federal crimes, including . . . [the wire
2 fraud and mail fraud statutes].” Congress provided a like directive to the U.S. Sentencing
3 Commission, instructing it to consider providing sentencing guideline enhancements for those
4 convicted of §1037 criminal spamming crimes who obtain e-mail addresses through improper
5 means including e-mail address harvesting and dictionary attacks, and who are also convicted of
6 other fraud offenses if they involve the sending of large quantities of e-mail.¹²

7 **Soloway’s Criminal Spamming and Fraud Scheme in the WD WA**

8 Enactment of federal anti-spam legislation, like passage of state anti-spam statutes before
9 it, did not deter Soloway from continuing spamming techniques that were in flagrant violation of
10 federal criminal (and civil) law as of January 1, 2004. Rather, Soloway persisted, after his move
11 to Washington, in what had then become federal spamming crimes. He did so to promote his
12 web-based “distribution e-mail” (spamming) business, which was itself a fraudulent business by
13 which Soloway sold spamming “products” and “services” based on numerous
14 misrepresentations.

15 **The Spam**

16 Soloway forged the “from” headers in his spammed advertisements, in clear violation of
17 18 USC 1037(a)(3). Soloway, moreover, committed that forgery in a particularly egregious
18 manner - rather than simply forging a false or non-existent name into a “from” header, he would
19 use identifiable names, e-mail addresses, and domain names that belonged to real people and
20 companies. This deliberate and conniving technique enhanced Soloway’s ability to avoid spam
21 filtering, and force his unwanted spam into many more victims’ systems.¹³ Not surprisingly, it
22 also caused outrage among victims who repeatedly saw evidence, in the form of Soloway’s
23 redundant spams, that he had stolen identifiers that belonged to them, for a criminal purpose.
24 These victims feared the impact that this criminal spamming might have on their own reputations

25
26 ¹²*Supra*, at 4(b) and (c).

27 ¹³ Exhibit E.

1 and businesses. And when these victims attempted to contact Soloway to instruct him to stop,
2 their requests were at best ignored; more often, rudely rebuffed.¹⁴

3 Soloway also used “protected computers”¹⁵ to relay or retransmit hundreds of millions of
4 his commercial, criminal forged spammed advertisements, in clear violation of 18 U.S.C.
5 §1037(a)(2). He did this by renting “server” computers, on which he would load the “Dark
6 Mailer” program.¹⁶ Dark Mailer enabled the use of a network of proxy computers to actually
7 send the spammed messages - thereby substituting the Internet Protocol (“IP” address) of these
8 proxies for that of his own computer as the source of the criminally spammed messages. By thus
9 substituting myriad other IP addresses for that of his own, Soloway was able by this technique,
10 too, to thwart spamming filters that make use of identified source IP addresses as an indicia of
11 unwanted spam. This was yet another way in which Soloway could force his unwanted spam
12 into the systems of even those who had attempted to be proactive to defeat it.

13 Soloway was also harvesting e-mail addresses, and routinely using “dictionary attack”
14 spamming techniques.¹⁷ And in perhaps the ultimate cynical demonstration of his fraudulent e-
15 mail intent, Soloway began representing in his criminally spammed advertising messages
16 themselves that they were “non-commercial,” and the “distribution e-mailing” advertised therein

17
18

19 ¹⁴Exhibit E. Numerous victims whose names or other identifiers were forged into “from” headers
20 also reported experiences of “bounced back” e-mails, indicating to them that their identifying e-mail
21 addresses and/or domain names had been forged into “from” headers used in advertisements that were
22 criminally spammed to others. At least one victim, R. Middleton, provided documentary evidence in
23 support of this claim by providing copies of criminally spammed messages that were transmitted to a
third address with headers that had been forged to appear as though he was the source of the criminal
spam. The government was able to corroborate, as part of its investigation, that Soloway had indeed
been hired to provide “distribution e-mail” on behalf of each of the companies advertised in these illegal
spam messages.

24 ¹⁵*i.e.*, other computers connected to the Internet.

25 ¹⁶SA Schmutz, FBI Analyst Ervin, and Mr. Collins of Liquid Web, will provide evidence in the
26 form of testimony and corresponding exhibits regarding Soloway’s use of Dark Mailer and proxies to
27 transmit his criminal spam. The government intends, in addition, to offer proof that the proxies used by
28 Soloway were “botnet” (hacked computer) proxies.

¹⁷Exhibit F.

1 was “. . . not a commercial offering and is not available for sale, lease, trade, or for use in any
2 commercial purpose or use of any kind”.¹⁸

3 **The Fraudulent “Distribution E-Mail” (Spamming) Business**

4 Soloway solely owned and operated the “distribution e-mail” business he promoted via
5 his criminal spamming. It was, in reality, a “spamming” business - Soloway sold a “product” to
6 enable others to send bulk commercial e-mail, i.e., making it possible for them to “spam”; and he
7 sold bulk commercial e-mailing (spam) “services,” (he would spam for customers, for a fee).
8 Both the product and service were offered for sale “on-line,” through websites published by
9 Soloway.

10 Soloway himself agreed, as part of his Plea Agreement, that he “made numerous false and
11 fraudulent misrepresentations on [his] online NIM websites regarding the ‘services’ and
12 ‘product’ that were there offered for sale,” including representations (beginning in May, 2006)
13 that the service and package sold consisted of “opt-in e-mail addresses,” that Soloway’s company
14 “provided ‘24/7 Customer and Technical Support Department with everything you need’; and
15 that if a purchaser of the product did “not receive at least a 400% increase in sales after using [the
16 product] for 90 days,” the customer could “simply return it . . . for a full 100% refund, no
17 questions asked.”¹⁹

18 The “numerous” fraudulent misrepresentations also included false statements about his
19 purported relationship with well-known charities, and his alleged “24/7 Easy Hassle-Free Email
20 Removal From Our [sic] All of Our Emailing Lists Upon Request”.²⁰ While Soloway admitted

21
22 ¹⁸Exhibit G. Soloway used many different variations of this “non commercial e-mail claim” for
23 the e-mails he criminally spammed to promote the website through which he earned almost \$1,000,000
24 in just over three years. [Note also the representation in this particular spammed message that “. . . this
25 non-commercial, non-transactional, non-relationship email originated from a computer outside of the
26 united states of america by a citizen of a foreign country and obeys all non-commercial email laws of the
27 country of the citizen that initiated this non-commercial email.” Soloway seems to be asserting (falsely)
28 thereby that the spam he transmits to U.S. residents (in violation of U.S. law) is not subject to U.S. law,
but only that of Sweden (the other country for which he holds citizenship).

¹⁹Plea Agreement, at 8-9.

²⁰Exhibit I.

1 as part of the Plea Agreement that he made misrepresentations regarding the refund policy for his
2 “product,” numerous victims additionally reported that Soloway harassed and threatened them
3 with extra fees, collection actions, and “7 years of bad remarks on their credit” if they
4 approached their credit card companies for refunds on either the product or service. As astutely
5 remarked by one such victim, Soloway defrauded his customers, and “[t]hen use[d] harassment
6 as the method to get you to not dispute their false advertising.”²¹

7 In sum, Soloway wasn’t just a criminal spammer, but a criminal spammer who used fraud
8 in e-mail to promote his own fraud scheme - a quintessential example of the Congressional
9 concern that spam is harmful not only because of the damage it does directly to Internet
10 communications and commerce, but also because it “. . .has become the method of choice for
11 those who . . . perpetrate fraudulent schemes.”

12 **Soloway Defied Attempts to Seek Legal Compliance Through Civil Actions**

13 As noted above, Congress specified that only certain limited entities - including ISPs -
14 could bring federal civil actions against those who commit e-mail fraud through spam. Two ISPs
15 - Microsoft, as owner of MSN Hotmail, and Robert Braver, the individual owner of a small ISP
16 in Oklahoma - elected to pursue civil litigation against Soloway in light of his voluminous,
17 relentless spamming activity. In each of these cases, significant damages were awarded by way
18 of default judgments against Soloway - \$7,845,000 to Microsoft in May, 2005, and a judgment of
19 \$10,075,000.00 was awarded Mr. Braver on September 22, 2005.²² By order of that same date,
20 United States District Court Judge Ralph Thompson permanently enjoined Soloway from:

21 a. Initiating the transmission of a commercial [e-mail] message, to any
22 computer involved in interstate commerce or communication, or a transactional or
23 relationship message, that contains, or is accompanied by, header information that
24 is materially false or misleading;

25 e. Relaying or retransmitting a commercial [e-mail] message that is
26 unlawful under 15 U.S.C. 7704(a) from a protected computer or network accessed
27 without authorization.

28 ²¹Exhibit J.

²²Exhibit K.

1 Remarkably, Soloway brazenly defied Judge Thompson’s permanent injunction every day
2 thereafter, until the day of his arrest some 15 months later. Nor has he ever made a payment to
3 either Microsoft, or Robert Braver in satisfaction of those judgments, despite the fact that he
4 continued to earn lucrative profits from the criminal spamming activities from which Judge
5 Thompson explicitly had enjoined him. Instead, Soloway actively evaded legal collection efforts,
6 and even publically boasted about it, proclaiming in an Internet posting that, “. . . I always win . .
7 . regardless of the judgment amount . . . losing is not an option, and I never ever, ever have to pay
8 a single cent to anyone . . . :)”²³

9 **IV. Argument: Sentencing Factors**

10 **A. Application of the Sentencing Guidelines Results in a Recommended Range
11 of 87 - 108 Months Imprisonment**

12 The Sentencing Guidelines remain the starting point for sentencing proceedings, and the
13 range “must be calculated correctly.” United States v. Carty, 520 F.3d 984, 991 (9th Cir. 2008).

14 The government believes the correct Guideline computation in this case to be as follows:

15 Base Offense Level (U.S.S.G. §2B1.1): 7

16 Specific Offense Characteristics:

17 Loss amount greater than \$400,000 (§2B1.1(b)(1)(G)): +14

18 Offense involved 250 or more victims (§2B1.1(b)(2)(A)(C)): +6

19 §1037 offense & e-mail addresses by improper means (§2B1.1(b)(7)): +2

20 Violation of prior specific Court Order (§2B1.1(b)(8)): +2

21 Adjusted Offense Level: 31

22 Potential Adjustment for Acceptance of Responsibility (§3E1.1(a)): -2

23 Total Offense Level, with Acceptance of Responsibility: 29

24 Based on an offense level of 29, and a criminal history category of I, the Guidelines yield a
25 recommended range of imprisonment of 87 to 108 months.

26
27
28 ²³Exhibit L.

1 **Loss Amount**

2 Loss amount is a challenging issue under the circumstances of this case - circumstances, it
3 should be emphasized, that are entirely of the defendant's making.

4 The challenge begins with the fact that Soloway committed two distinct fraud crimes,
5 which have each resulted in significant, but very different types of losses. First, as to his fraud in
6 e-mail, (criminal spamming) crimes, evidence - as well as reason and common sense - supports a
7 finding that there were pecuniary losses (albeit sometimes very small) to hundreds of millions of
8 Internet users, worldwide, who for years were forced to spend, at a minimum, their valuable time
9 to assess and remove Soloway's uninvited and unwanted criminal spam from their systems. This
10 loss of time and productivity is a real and a pecuniary harm to all Internet users, and necessitates
11 other costs in the form of spam filtering services and hardware solutions. The Court should
12 specifically recognize these very real and significant losses, and reject Soloway's attempts to
13 minimize them, and demean the victims who rightfully complain of them. Difficulty in
14 quantifying them is not grounds for pretending they do not exist, and only serves to embolden the
15 criminal spammers whose lucrative profits are generated in proportion to the costs they impose on
16 their victims. For the same reason, the Court should specifically address and make a finding
17 regarding the significant losses caused to all ISPs and the infrastructure of the Internet by
18 Soloway's criminal spamming. Beyond the generalized losses experienced by all Internet users
19 and ISPs, moreover, there is an abundance of evidence in this case regarding actual pecuniary
20 losses, that are quantifiable, on the part of small business people such as Mr. Corbalis and Mr.
21 Reel, or non-profit agencies, such as the Santa Barbara Dept. of Social Services. Soloway's
22 malicious and persistent spamming cost them tens of thousands of dollars in expenses that
23 Congress mandated be included in "loss" computations for §1037 offenses.

24 Soloway's fraudulent "distribution e-mail" business caused losses of other types to other
25 victims - the money the customers paid Soloway under false pretenses, but also the "reasonably
26 foreseeable" pecuniary harms that resulted after those purchases were made, including damages
27 that flowed from the loss of e-mail accounts or websites that were shut down after being
28

1 associated with spam. As among these losses, some are readily quantifiable (the price paid for the
2 product); others not. But again, the difficulty in quantifying them should not be grounds for
3 allowing Soloway - or any other perpetrator of fraud - to evade responsibility for them at
4 sentencing.

5 The court “is not required to calculate loss ‘with absolute precision’,” and “need only
6 make a reasonable estimate of the loss based on the available information.” United States v. Zolp,
7 479 F.3d 715, 719 (9th Cir. 2007); United States v. Santos, F.3d __, 2008 WL 2312391 (9th Cir.
8 6/6/2008). Factors that can be included in such an estimate are the “approximate number of
9 victims multiplied by the average loss to each.” *Application Note 3.(C)(iii), Commentary*, USSG
10 §2B1.1. And, in those cases in which there is a loss, but it “reasonably cannot be determined,” the
11 Guidelines provide, and the Courts have endorsed “the gain that resulted from the offense as an
12 alternative measure of loss.” *Application Note 3.(B)*. United States v. Canova, 412 F.3d 331 (2nd
13 Cir. 2005). See also: United States v. Lamoreaux, 422 F.3d 750, 756 (8th Cir. 2005) (affirming
14 use of defendant’s gain as an alternate measure of loss where defendant convicted of mail fraud
15 based on his negotiating and receiving commissions from employer’s supplier without employer’s
16 knowledge); United States v. Munoz, 430 F.3d 1357, 1369-1371 (11th Cir. 2005) (defendant’s
17 sentence properly increased based on his gain where defendant convicted of mail fraud in
18 connection with advertising and distributing misbranded drugs without a prescription; many
19 factors made a precise calculation of loss uncertain and defendant’s gain would not underestimate
20 the loss). This was, in fact, the approach adopted by United States District Court Judge Lewis
21 Babcock, District of Colorado, in sentencing the defendant in a criminal spamming case in that
22 district in November, 2007.²⁴

23 The gain that resulted to Soloway, as measured by the invoices he himself issued for the
24 sale of his fraudulent “distribution e-mail” product and service, is also consistent with, and bears a
25 direct relationship to “intended loss.” United States v. Lucas, 516 F.3d 316, (5th Cir. 2006) (in
26

27 ²⁴Exhibit M.
28

1 mail fraud prosecution arising from fraudulent sale of mobile home lots, sale price of lots could be
2 used to calculate amount of money defendant intended to receive from fraud, and in turn, amount
3 of loss to victims, for sentencing purposes). *See also: United States v. Santos*, __ F.3d __, (9th Cir.
4 2008), in which the Ninth Circuit recently endorsed the inference drawn, by the district court, that
5 the defendant's intended loss in a fraud case equaled the face value of the checks he had stolen,
6 and thus could properly be used as the "loss" amount for sentencing purposes.

7 As part of the Plea Agreement, the parties agreed that Soloway "relocated" to Washington
8 from Oregon "on or about March 18, 2004." The 5,817 invoices issued by Soloway for the period
9 from March 18, 2004 until May 30, 2007, total \$931,555. Bank records reflecting bank deposits
10 by Soloway during the period of January 1, 2004, through December, 2006, show deposits of
11 \$813,820.54.²⁵ Adopting either of these figures as loss, (based either on "gain," or "intended
12 loss"), represents a reasoned and appropriate loss determination for purposes of calculating the
13 appropriate Sentencing Guideline range under the circumstances of this case. And using either
14 approach, the loss amount for sentencing purposes is between \$400,000.00 and \$1,000,000. The
15 government respectfully submits that a loss figure that is any less would not represent a correct
16 calculation of loss in this case.

17 **Number of Victims**

18 Application Note 4.(B) of the Commentary to USSG 2B1.1 specifically addresses the
19 "victim number" enhancement in criminal spamming cases, and provides thereby that such cases
20 "shall be considered to have been committed through mass-marketing," so that "the defendant
21 shall receive at least a two-level enhancement . . . and may, depending on the facts of the case,
22 receive a greater enhancement under [the victim number enhancement] if the defendant was
23 convicted under . . . 18 U.S.C. § 1037." (Emphasis added.) The facts of this particular case are
24 such that a greater enhancement - that for "250 or more victims" - is warranted and proper.

25
26
27 ²⁵Bank records are only available up through December of 2006, because that was the time at
28 which they were subpoenaed for the investigation.

1 Soloway has proudly proclaimed himself to be “Top 10 E-Mailer in the World,”²⁶
2 and the evidence in this case establishes, without question, that he was responsible for uninvited
3 criminal spams numbering in the hundreds of millions - (and likely billions) - to Internet users,
4 worldwide, for years. The purpose of these criminal spams was the promotion and sale of
5 spamming products and services from his own fraudulent company. Naive customers were led to
6 believe that what he was offering was “legitimate,” and shocked when they were subsequently
7 identified as “spammers.” Doubtless, Soloway also had customers who understood that what he
8 was offering was spamming (and address harvesting) capabilities, and were indifferent to that fact
9 so long as they gained the ability to clog the Internet, and unwilling recipients’ systems, with their
10 own (also possibly fraudulent) spam.

11 This is a case in which a mere “2 point” enhancement - the same enhancement made for
12 “10 or more victims” - is wholly inadequate and flatly at odds with the facts, as well as reason and
13 common sense. Soloway’s spamming victims - all of whom suffered at least some (even if small)
14 pecuniary harm - numbered in the hundreds of millions, or billions. He sold his fraudulent
15 product and service to thousands. He continued to persist in each of these criminal pursuits
16 relentlessly, despite the many complaints and protestations made by hundreds of his victims.

17 The Probation Office has suggested that a “2 point” victim adjustment is proper, because
18 “a tremendous majority of recipients of those emails are not considered victims under the
19 guidelines as they suffered no economic loss.” (PSR, at paragraph 61). The Probation Office
20 seems to reach this conclusion because less than 49 victims have filed written statements
21 certifying a sum certain as loss, for purposes of restitution. The statute that provides for
22 restitution procedures specifically states, however, that “[n]o victim shall be required to
23 participate in any phase of a restitution order.” 18 U.S.C. §3664(g)(1). A victim’s election to file,
24 or not file a loss statement for restitution purposes is a statutory right they are accorded, and their
25 election not to seek restitution should not be a basis for excluding them from consideration as a
26 “victim” in calculating the impact of the crime for sentencing purposes. This would represent an
27

28

²⁶Exhibit L.
SENTMEMO/Soloway, Robert, CR07-187MJP
Page 16

1 (unstated) penalty, of sorts, flowing from an exercise of their statutory right not to file a restitution
2 claim.

3 A victim enhancement of any less than the “6” routinely provided in any case involving
4 more than 250 victims, does not properly reflect, nor respect, the millions of victims of Soloway’s
5 criminal spamming, and fraud conduct.

6 **B. Factors Under § 3553(a) Support a Sentence of 108 Months Imprisonment,
7 Which is Also a “Reasonable” Sentence**

8 While the Sentencing Guidelines are a starting point, “the overarching statutory charge for
9 a district court is to ‘impose a sentence sufficient, but not greater than necessary’ that accounts for
10 all of the factors identified in 18 U.S.C. § 3553. United States v. Carty, *supra*, at 991. The
11 government contends that these factors, even more than the Guidelines, support a sentence of 108
12 months under the aggravated circumstances of this particular case, and intends to articulate its
13 reasons in further depth at the sentencing hearing. Those aggravating factors take this case well
14 out of the “heartland” of offense conduct addressed by the Sentencing Guidelines.

15 **C. Forfeiture**

16 Subsection (c) of § 1037 provides that the Court “shall order” that Soloway forfeit to the
17 United States “any property, real or personal, constituting or traceable to gross proceeds obtained
18 from” his criminal spamming offense. Soloway’s criminal spamming continued from the day he
19 moved to Washington, until the day he was arrested, and it’s sole purpose throughout was to
20 advertise and promote his fraudulent business. The gross proceeds from that operation are
21 forfeitable, in their entirety, to the United States.²⁷

22
23
24
25 ²⁷18 U.S.C. § 1037(c)(2) provides that “[t]he procedures set forth in section 413 of the Controlled
26 Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal
27 Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this
28 section.” Rule 32.2(b)(1), in turn, provides for the imposition by the Court of a personal money
judgment. (“If the government seeks a personal money judgment, the Court must determine the amount
of money that the defendant will be ordered to pay. The Court’s determination may be based on evidence
already in the record, including any written plea agreement, or, if the forfeiture is contested, on evidence
or information presented by the parties at a hearing after the verdict or finding of guilt.”)

1 **D. Restitution**

2 Consistent with the terms of 18 U.S.C. §3664, the government requests that a date be set
3 for the final determination of restitution, not to exceed 90 days after sentencing.

4 **E. Allocation of Sentence**

5 Assuming the defendant has accepted responsibility for his conduct at the time of
6 sentencing, the government will request a sentence of 108 months imprisonment, and further
7 request that 60 months of that sentence be imposed specifically for the §1037 criminal spamming
8 conviction. Sixty months is the maximum sentence available for that offense, and the government
9 contends that the facts of this case warrant the maximum possible penalty.

10 **F. The Sentence Should Include 624 Hours of Community Service to be**
11 **Performed During Supervised Release, as well as Restrictions on Internet Access During**
Supervised Release

12 Soloway has boasted publically that he will “never ever, ever have to pay a single cent to
13 anyone” as the result of court actions, and his family circumstances may well enable him to stay
14 true to this boast by obviating the need for any future wage-earning employment. The Court can,
15 however, insure that Soloway makes a contribution to the public he has abused and defrauded
16 through a requirement of community service. The government proposes a mere four hour per
17 week obligation - for a total of 624 hours of community service during his three years of
18 supervised release.

19 A prohibition on access to the Internet, at any location (including employment) without the
20 prior written approval of the Probation Office, is also appropriate and warranted. Under the facts
21 of this case, such a condition is reasonably related to the goal of deterrence, protection of the
22 public, and rehabilitation of the offender, and involves no greater deprivation of liberty than is
23 reasonably necessary for the purposes of supervised release. United States v. Rearden, 349 F.3d
24 608, 618 (9th Cir. 2003).

25 **V. Conclusion**

26 On the grounds and for the reasons set forth above, the United States urges imposition of a
27 sentence of 108 months imprisonment, followed by three years of supervised release, including
28

1 624 ours of community service. Further, the United States seeks a preliminary order of forfeiture
2 for all proceeds of Soloway's criminal spamming, or for substitute assets to satisfy any money
3 judgment of forfeiture. Finally, the United States asks for conditions of supervision that include
4 624 hours of community service, and restrictions, under Probation supervision, for computer and
5 Internet access.

6 Dated this 7th day of July, 2008.

7 Respectfully Submitted,

8
9 JEFFREY C. SULLIVAN
10 United States Attorney

11 /s/Kathryn Warma

12 KATHRYN WARMA
13 Assistant United States Attorney
14 700 Stewart Street, Suite 5220
15 Seattle, Washington 98101-1271
16 Phone: (206) 553-8786
17 Fax: (206) 553-2502
18 Email: KWarma@usdoj.gov

19 /s/Richard E. Cohen

20 RICHARD E. COHEN
21 Assistant United States Attorney
22 700 Stewart Street, Suite 5220
23 Seattle, Washington 98101-1271
24 Phone: (206) 553-2242
25 Fax: (206) 553-6934
26 Email: Richard.E.Cohen@usdoj.gov

1 **CERTIFICATE OF SERVICE**

2 I HEREBY CERTIFY that on July 7, 2008 I electronically filed the foregoing with the
3 Clerk of the Court using the CM/ECF system, which will send notification of such filing to the
4 attorney(s) of record for the defendant(s). I hereby certify that I have served the attorney(s) of
5 record for the defendants(s) that are non CM/ECF participants via telefax.
6

7 s/Kimberly King
8 KIMBERLY KING
9 Legal Assistant
10 United States Attorney's Office
11 700 Stewart Street, Ste. 5220
12 Seattle, Washington 98101
13 Phone: (206) 553-5127
14 Fax: (206) 553-2502
15 E-mail: Kimberly.King3@usdoj.gov
16
17
18
19
20
21
22
23
24
25
26
27
28