LEXSEE 2007 U.S. DIST. LEXIS 63172

United States of America, Plaintiff, vs. Jeffrey A. Kilbride (2), James R. Schaffer (3), Defendants.

CR 05-870-PHX-DGC

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF ARIZONA

2007 U.S. Dist. LEXIS 63172

August 24, 2007, Decided
August 24, 2007, Filed

PRIOR HISTORY: *United States v. Kilbride, 2007 U.S. Dist. LEXIS 40471 (D. Ariz., June 1, 2007)*

COUNSEL: [*1] For Jeffrey A Kilbride (2), Defendant: Steven M Goldsobel, LEAD ATTORNEY, Law Office of Steven M Goldsobel, Los Angeles, CA.

For USA, Plaintiff: Bonnie Lynne Kane, Kayla Bakshi, LEAD ATTORNEYS, US DOJ, Child Exploitation & Obscenity Section, Washington, DC; Jill Rochelle Trumbull-Harris, LEAD ATTORNEY, US DOJ, Criminal Division, Washington, DC; John Robert Lopez, IV, LEAD ATTORNEY, US Attorney's Office, Phoenix, AZ.

JUDGES: David G. Campbell, United States District Judge.

OPINION BY: David G. Campbell

OPINION

ORDER

On June 25, 2007, following three weeks of trial, the jury returned a guilty verdict against Defendants Jeffrey A. Kilbride and James R. Schaffer. The jury found Defendants guilty of conspiracy to violate the *CAN-SPAM Act of 2003* (Count 1), criminal violations of the CAN-SPAM Act (Counts 2 and 3), interstate transportation of obscene material (Counts 4 and 5), interstate transportation of obscene material for sale (Counts 6 and 7), and conspiracy to commit money laundering (Count 8). Dkt. # 296. Defendant Kilbride has filed a motion for judgment of acquittal under *Rule 29 of the Federal Rules of Criminal Procedure* or, alternatively, for a new trial under *Rule 33*. Dkt. # 301. Defendant Schaffer has joined [*2] the motion. Dkt. # 327. Responses and replies have been filed. Dkt. ## 320, 333.

The parties have informed the Court that this was one of the first, if not the first, criminal trials under the CAN-SPAM Act. Defendants' motion calls upon the Court to address several novel issues regarding that statute. The Court will first provide background information concerning this case and the charges brought by the Government. The Court will then address Defendants' arguments concerning the counts of their conviction. The Court will conclude by addressing Defendants' argument that Juror 16 should have been excused. For reasons the Court will explain, Defendants' motion for acquittal or a new trial will be denied.

I. BACKGROUND.

Defendant Jeffrey Kilbride is a resident of California. Defendant James Schaffer is a resident of Arizona. Since at least 2003, Kilbride and Schaffer have been engaged in the business of sending large volumes of unsolicited commercial emails, commonly referred to as "spam," containing pornographic images. When a recipient opened one of Defendants' emails the sexually explicit images of a pornographic Internet website would instantly appear on the recipient's computer screen. [*3] If the recipient signed on to the pornographic website and paid a fee, Defendants would earn a commission.

Defendants' business was lucrative. A Government

expert testified that Defendants earned $ 1,417,161 in the year 2003 from their spam email operation. Defendants achieved this level of income by sending literally millions of unsolicited pornographic emails to persons throughout the United States and the world.

In an attempt to curb the abuses of spam emails, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketings Act of 2003, commonly known as the "CAN-SPAM Act." *15 U.S.C. §§ 7701-7713*; *18 U.S.C. § 1037*; Pub. L. 108-187, 117 Stat. 2699 (2003). The Act was intended to prohibit senders of spam "from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages." S. Rep. No. 108-102, at 1 (2003).

The CAN-SPAM Act did not make the mere sending of bulk emails a crime. Congress acted more narrowly. For purposes of this case, two provisions of the Act are relevant. First, Congress prohibited the sending of bulk commercial emails that contain materially false header information. *18 U.S.C. § 1037(a)(3)*. [*4] Second, Congress prohibited the sending of bulk commercial emails from accounts or domain names registered using materially false information. *18 U.S.C. § 1037(a)(4)*. Each provision includes an element of fraud. Indeed, the title of *§ 1037* is "Fraud and related activity in connection with electronic mail."

The CAN-SPAM Act became effective on January 1, 2004. Defendants were well aware of the Act and its effective date. As the evidence recounted below will demonstrate, Defendants acted to move their email operation overseas by the effective date and to disguise their involvement with the operation, even while they continued to send the pornographic emails from a computer located in Defendant Schaffer's Arizona home.

II. COUNT 1 - CONSPIRACY TO VIOLATE THE CAN-SPAM ACT.

Count 1 charges Defendants with conspiracy to violate the CAN-SPAM Act. Defendants argue that the count is defective because it fails to allege that the conspiracy had an illegal objective. True, to be guilty of conspiracy Defendants must have conspired "to commit an[] offense against the United States." *18 U.S.C. § 371*. Contrary to Defendants' assertion, however, the Indictment did allege an illegal objective.

The opening [*5] paragraph of Count 1 alleges that Defendants conspired to violate the two fraud provisions of the CAN-SPAM Act described above:

> [Defendants] did knowingly conspire with one another to knowingly falsify header information in multiple commercial electronic mail messages, and intentionally initiate the transmission of such messages, in violation of Title *18, United States Code, Section 1037(a)(3)*, and to knowingly register, using information that materially falsified the identity of the actual registrant, for two or more domain names, and intentionally initiate the transmission of multiple electronic mail messages from this combination of domain names, in violation of Title *18, United States Code, Section 1037(a)(4)*.

Dkt. # 1.

Defendants note that the section of the Indictment titled "Object of the Conspiracy" did not refer to a CAN-SPAM violation, but instead stated that Defendants engaged in the business of sending bulk pornographic email messages. *Id.* Defendants also note that the Government frequently referred during trial to Defendants' "porn-spam" conspiracy. Defendants argue that these ambiguities led the jury to convict Defendants of conspiracy to engage in perfectly legal activity [*6] - sending bulk commercial pornographic emails.

The Court does not agree. As noted above, the Indictment specifically alleged that Defendants conspired to violate two fraud provisions of the CAN-SPAM Act. The Court views these allegations as sufficient, particularly given Defendants' failure to challenge the adequacy of Count 1 before trial. Indictments are to be given a liberal construction when challenged for the first time post-trial. *See United States v. Ross, 206 F.3d 896, 899 (9th Cir. 2000)*; *United States v. Pheaster, 544 F.2d 353, 361 (9th Cir. 1976)*.

Moreover, there was no ambiguity in the Court's jury instructions. Instruction 21 provided the following explanation of the conspiracy charge:

> Count One of the indictment specifically

> charges defendants Jeffrey A. Kilbride and James R. Schaffer with conspiring to commit the following two crimes: First, knowingly materially falsifying header information in multiple commercial electronic mail messages, and intentionally initiating the transmission of such messages, in violation of Title *18, United States Code, Section 1037(a)(3)*. Second, knowingly registering two or more domain names using information that materially falsified the identity [*7] of the actual registrant, and intentionally initiating the transmission of multiple commercial electronic mail messages from these domain names, in violation of Title *18, United States Code, Section 1037(a)(4)*.

Dkt. # 330. The Court further instructed the jury that Defendants could be found guilty of conspiracy only if there was "an agreement between two or more persons to commit at least one of the two crimes I have just described[.]" *Id.*

The verdict form was clear as well. It described Count 1 as "Conspiracy to Violate *18 U.S.C. §§ 1037(a)(3)* and *1037(a)(4)*." Dkt. ## 296, 297.

Although the Government did refer to a "porn-spam" conspiracy during trial, the Court is confident that the jury did not misunderstand the Government's meaning or the requirements of Count 1. Defendants repeatedly noted during trial, through numerous witnesses, that sending bulk pornographic email is not illegal. The evidence focused on false header and registration information. And the Government clearly argued in closings that there was an agreement between Defendants and others "to commit at least one of the two CAN-SPAM Act violations alleged in Counts 2 and 3." Dkt. # 319-13 at 9.

III. COUNT 2 - VIOLATION OF CAN-SPAM ACT *§ 1037(a)(3)*.

Count [*8] 2 charges Defendants with violating *18 U.S.C. § 1037(a)(3)*. Defendants argue that the evidence failed to prove such a crime. The Court disagrees.

A. *Section 1037(a)(3)*.

Section 1037(a)(3) makes it a crime for any person to knowingly "materially falsif[y] header information in multiple commercial mail messages and intentionally initiate[] the transmission of such messages[.]" There is no dispute that Defendants intentionally transmitted multiple commercial emails. The question for purposes of this motion is whether Defendants materially falsified header information in those emails.

Under the CAN-SPAM Act, "header information" means "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." *15 U.S.C. § 7702(8)*. [1]

> 1 The CAN-SPAM Act contained both civil and criminal provisions. This definition is found in the civil provisions, but is incorporated by reference in the criminal provisions. *See 18 U.S.C. § 1037(d)(4)*.

Materially false information is defined in the [*9] Act as follows:

> [H]eader information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

18 U.S.C. § 1037(d)(4).

This definition focuses on hiding any person "who initiated the electronic mail message." *Id.* Thus, in applying the Act, the identity of the person initiating the email will be important. To "initiate" means "to originate or transmit [an email] message or to procure the origination or transmission of such message[.]" *15 U.S.C. § 7702(9)*. To "procure" another person to initiate an email means "to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf." *15 U.S.C. § 7702(12)*. The Act makes clear that "more than one person may be considered to have initiated a message." *15 U.S.C. § 7702(9)*.

The Court provided each of these definitions to the jury as part [*10] of the final jury instructions. Dkt. # 330, Instruction 26. Applying the definitions, the Court now concludes that the Government presented sufficient evidence to show that Defendants initiated and procured the initiation of millions of spam emails, and that the source information, routing information, and other information purporting to identify the initiator of those emails was altered or concealed in a manner that impaired the ability of the email recipients, Internet Service Providers ("ISPs"), and others to identify, locate, and respond to Defendants as the initiators. [2]

> 2 An Internet Service Provider or ISP is a business or organization that offers Internet services to consumers such as email and general Internet access. America On-Line ("AOL") is a well-known ISP referred to in this order. ISPs are referred to in the CAN-SPAM Act as "Internet access services." *See 15 U.S.C. § 7702(11)*; *see also 47 U.S.C. § 231(e)(4)*.

B. Evidence Presented by the Government.

Under *Rule 29*, the Court "must enter a judgment of acquittal on any offense for which the evidence is insufficient to sustain a conviction." *Fed. R. Crim. P. 29(a)*. "The evidence is sufficient to support a conviction if 'viewing [*11] the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *United States v. Milwitt, 475 F.3d 1150, 1154 (9th Cir. 2007)* (quoting *Jackson v. Virginia, 443 U.S. 307, 319, 99 S. Ct. 2781, 61 L. Ed. 2d 560 (1979)*).

Under *Rule 33*, "the court may vacate any judgment and grant a new trial if the interest of justice so requires." *Fed. R. Crim. P. 33(a)*. "'A district court's power to grant a motion for a new trial is much broader than its power to grant a motion for judgment of acquittal.'" *United States v. Kellington, 217 F.3d 1084, 1097 (9th Cir. 2000)* (quoting *United States v. Alston, 974 F.2d 1206, 1211 (9th Cir. 1992))*. "The court is not obliged to view the evidence in the light most favorable to the verdict, and it is free to weigh the evidence and evaluate for itself the credibility of the witnesses." *Id.* If the Court applying this standard concludes that the verdict is against the weight of the evidence, a new trial may be granted.

Applying both rules, the Court concludes that Defendants' convictions should be sustained. The discussion of the evidence that follows, although a necessarily incomplete recounting [*12] of three weeks of evidence, fairly represents the Court's view of the facts established during trial. The facts are not merely stated in the light most favorable to the Government. Rather, the following description represents the Court's view of the fair import of the evidence considering witness credibility. As this description will reveal, the evidence against Defendants was substantial and convincing.

The Government presented testimony from three of Defendants' employees who have pleaded guilty to crimes arising from Defendants' email operations and two of Defendants' overseas business affiliates who testified under grants of immunity. The Government also presented testimony from computer and financial experts and introduced scores of exhibits, including extensive bank records.

1. Andrew Ellifson.

Andrew Ellifson is a computer network specialist. In approximately April of 2003, Ellifson set up a network of computer servers in Amsterdam, The Netherlands, in anticipation of future business opportunities. Ellifson met Defendants Kilbride and Schaffer in early 2003 and eventually became the paid administrator of their email computer network.

After meeting Defendants in the Spring of 2003, [*13] Ellifson testified that he met with Defendant Schaffer again in approximately June. Schaffer told Ellifson that Schaffer and Kilbride wanted to use computers outside the United States to send emails. Ellifson told Schaffer about his Amsterdam network.

In October of 2003, Schaffer told Ellifson that Defendants wanted to use the Amsterdam network to avoid a law known as the CAN-SPAM Act that was being pushed through Congress. Defendants began using Ellifson's Amsterdam network to send emails in December of 2003. This use continued throughout 2004 and into 2005. Ellifson confirmed that he worked with Kilbride and Schaffer to evade the CAN-SPAM Act.

Ellifson presented evidence that Defendants sought to hide their involvement in the pornographic email operations. For example, in late 2003 Kilbride sent Ellifson and others an article regarding a new California law regulating emails. In the email forwarding this

article, Defendant Kilbride said that the new law demonstrated why Defendants needed to be "extremely careful in covering our tracks." Ex. 515.

Ellifson set up the means for Defendants to obtain remote access to the Amsterdam network from their homes in the United States. Ellifson testified [*14] that remote use of the Amsterdam computers to send emails would create the appearance that the emails were coming from outside the United States.

After hiring Ellifson to work for them, Defendants asked Ellifson to sign a consulting agreement with an entity known as The Compliance Company ("TCC"). This company was owned by Christopher Compston, an affiliate of Defendants from the Isle of Man. Ellifson never worked for TCC, but Defendants paid his monthly salary through this entity.

After Defendants had agreed to use Ellifson's Amsterdam computer network and had been granted remote access, Ellifson asked if they wanted their names on the network so they could obtain physical access. Kilbride stated that he did not want his name or Schaffer's to be affiliated with the Amsterdam network.

Ellifson owned and operated a Wisconsin corporation named Kobalt Network LLP. The corporation had no other owners or employees. Kobalt owned the domain name "knllc.net." The IP addresses used to send messages from the Amsterdam network were registered to Kobalt.

2. Christopher Compston.

Christopher Compston is a citizen of the Isle of Man. Compston testified that he was contacted by Kilbride in 2003 and asked [*15] to assist Kilbride in moving Kilbride's business operations offshore. Kilbride said he was running an email marketing business with Schaffer and expected to earn $ 1 million in annual profits. Kilbride said he wanted to move the operation offshore to avoid e-commerce regulations, including legislation about to be enacted in the United States.

Compston agreed to assist. He introduced Kilbride to Inter-Ocean Management ("IOM"), a business located in the country of Mauritius. Compston began acting as liaison between Kilbride and IOM, a service for which he received $ 2,000 to $ 2,500 per month.

With the assistance of IOM, Defendants used Compston to establish a company in Mauritius known as Ganymede Marketing. Although Ganymede was to be the entity through which Kilbride and Schaffer conducted their email pornography business, it was organized in a manner that obscured their involvement. The directors of Ganymede were not Kilbride and Schaffer, but Compston and Laval Law, an IOM employee. The owner of Ganymede was Lightspeed Holding Trust ("LHT"), of which Compston was the settlor. Two additional trusts - LBFM Ventures Trust and PJ Investment Group Trust - were the beneficiaries of LHT. [*16] Defendants were the beneficiaries of LBFM and PJ Investment Group.

Despite the fact that Compston and Law were the directors of Ganymede on paper, the company was controlled by Defendants. Kilbride directed its business operations and financial transactions through Compston. Compston testified during trial that his job was to "fulfill the wishes" of Kilbride. Compston further testified that nothing prevented Kilbride and Schaffer from appearing on the Ganymede documents or on Ganymede bank accounts, but that Kilbride made clear that he and Schaffer did not want to be linked to Ganymede.

Compston had another business - TCC. After Compston began working with Kilbride in the creation and operation of Ganymede, Kilbride asked Compston to set up a series of consulting agreements between TCC and various employees of Kilbride and Schaffer, including Andrew Ellifson, Kirk Rogers, and Jennifer Clason. None of these employees actually worked for TCC, but Kilbride provided contracts stating that they did. Kilbride thereafter directed that funds be transferred from Ganymede to TCC to be paid to these individuals. Kilbride told Compston that he did not want his employees working for Ganymede.

Compston [*17] explained that Kilbride was responsible for managing the business operations and finances of the enterprise, Schaffer was responsible for sending the pornographic emails, Ellifson managed the computer network, and Jennifer Clason was Schaffer's personal assistant in sending the emails. Kirk Rogers was also involved, although Compston was not sure what he did.

That Kilbride wanted no apparent association with Ganymede was abundantly clear from the evidence. Compston testified that Kilbride told Compston that Kilbride was not to be contacted by anyone in connection

with Ganymede, other than Compston. In October of 2004, Kilbride received a direct telephone call from an individual named John Mcllraith asking Kilbride questions about Ganymede. Kilbride responded with an angry and profane email to Compston demanding to know why he had been called with questions about Ganymede. Kilbride asked if the caller was an "idiot" and why the caller had no sense of Kilbride's "privacy concerns," stating that "[p]hone calls from [Mauritius] don't look good on my phone bill." Ex. 104. In other emails, Kilbride stated that he was reluctant to tie himself to Ganymede through a U.S. law firm and that his [*18] LBFM email address was not to be used in connection with Ganymede. Ex. 85, 57.

To complete the move of their business off-shore, Defendants transferred a large amount of money to Ganymede in late 2003. Because Kilbride did not want the transfer to go directly to Ganymede, he transferred it first to another Compston entity known as Cardpro, and from Cardpro to Ganymede. To create a paper justification for the transfer to Cardpro, Kilbride instructed Compston to create bogus invoices showing that Cardpro had sold email addresses to Kilbride's U.S. operation. No such sales had occurred.

At one point in the relationship, Kilbride asked Compston to contact an entity known as DirectNic and register domain names for Ganymede. Kilbride asked Compston to pay the registration fee with a credit card from TCC. In registering the domain names with DirectNic, Compston used his own name as the contact person for Ganymede. When Compston subsequently began receiving complaints about pornographic emails that were sent using the domain names he had registered, Compston became upset and contacted Kilbride. Kilbride said he was surprised Compston had used his true identity as the Ganymede contact person. [*19] Kilbride fixed the problem by contacting DirectNic and changing the contact person from Compston to Harry Plimpton (a fictitious name), the phone number from Compston's phone to a bogus phone number, and the contact email address so that emails went through Ganymede to Kilbride, rather than to Compston. Ex. 27. In doing so, Kilbride falsified the contact information for anybody trying to get in touch with Ganymede.

Thereafter, Kilbride assumed responsibility for registering Ganymede domain names, but he did so using the credit card of TCC. Ex. 83. Compston testified that Kilbride never used a credit card that could be traced to Kilbride or Schaffer.

During the operation of Ganymede, Kilbride periodically directed Compston to transfer funds to the trusts of which Kilbride and Schaffer were beneficiaries. Compston sometimes sent money directly to the trusts, forgoing LHT, the parent trust of Ganymede.

At one point in the relationship, Kilbride asked Compston for a name that could be used in registering domain names. Compston gave Kilbride the name of Chad Smith, a car salesman Compston knew. Kilbride used Smith's name in conducting business on behalf of Ganymede.

3. Laval Law.

Laval Law is [*20] a citizen of Mauritius. He has been employed by IOM since 2000. He was a director of Ganymede, but never met Kilbride or Schaffer. All communications with these individuals were directed through Compston.

Law testified that there is no Harry Plimpton associated with Ganymede. He has never heard of such an individual and knows that no such person has ever been employed by the company. Thus, when Kilbride changed the Ganymede contact person to Harry Plimpton, he was using a false name.

Law became a director of Ganymede because it is customary for IOM to designate one of its employees as a director of client companies. Law understood that Ganymede's business was internet marketing and website construction, but he did not know Ganymede was involved in advertising hard core pornographic websites. He first learned this fact in September 2004, many months after Ganymede had commenced operations. Law testified that he never would have agreed to serve as a director had he known Ganymede was involved in the pornography business.

When money was transferred to Ganymede from Cardpro in late 2003 and early 2004 for the alleged sales of email addresses, Law believed that the sales had actually occurred. [*21] He did not know that this was a bogus transaction created to enable Kilbride and Schaffer to place money in Ganymede.

The Government placed in evidence a large number

of emails between the operators of various pornographic websites and an individual purporting to be Laval Law. Exs. 338-351. Law testified that he was not a party to any of these emails. The emails were retrieved from Defendants' work stations in Amsterdam and showed that Defendants, primarily Schaffer, posed as Laval Law when communicating with pornographic website operators. Law never authorized Defendants to use his name in this fashion.

4. Kirk Rogers.

Kirk Rogers is a computer programmer. He was hired by Kilbride and Schaffer in February of 2003 to perform programming functions in connection with their commercial email business. Rogers testified that the business originally was based in Phoenix, but was moved to Amsterdam at the end of 2003. Rogers received $ 4,000 every two weeks for his work for Defendants.

Rogers explained the email system he helped create for Kilbride and Schaffer. The system was largely automated and was used to send emails to a vast number of addresses. These emails contained pornographic images [*22] and links to pornographic websites. Rogers explained that his program initially had 17 million email addresses, but eventually was expanded to between 30 and 35 million email addresses Defendants could use for their spam operation. Department of Justice computer expert James Fotrell later testified that 43 million email addresses were found on the computers used by Defendants.

Rogers testified that, at Defendants' direction, he added a feature to the program that allowed Defendants to send emails to individuals who had asked to be removed from Defendants' email lists. The program was designed so that every 30 days pornographic emails would be sent again to individuals who had requested that their names be removed.

The program had a "from" domain name which would show who had sent the email. This name, according to Rogers, could be changed at will. It was changed often, usually on a daily basis. Thus, when individuals who had requested to be removed from Defendants' email list received another email from Defendants, it typically would be shown as coming from a different domain name. Recipients would not know they were receiving an email from the same individuals who had originally sent [*23] them the pornographic emails and to whom they had directed a request for deletion from the email list.

Rogers testified that the program was also designed to take the user name of the person receiving the email and put it in the user name space of the return path. (The return path, as explained by expert witness Richard Kaplan, is the email address from which the email message is sent.) Rogers explained that the remainder of the return path would reflect the domain name that was changed randomly by Defendants and used in sending the email. Thus, if Defendants sent a pornographic email using the domain name "shoulderticks.com" and the email was received by an individual with the email address of "trresa@aol.com," Rogers' program would take the username of the recipient ("trresa") and combine it with the domain name used by Defendants in sending the email ("shoulderticks") and show a return path for the email of "trresa@shoulderticks.com." Dkt. # 319-13. Rogers testified that this device made it hard for recipients to determine who was sending the emails.

Rogers also testified that, at the direction of Defendants, his program allowed the sender to place additional text in the emails to [*24] avoid ISP spam filters. The program would swap out domain names frequently, making it difficult for an ISP to track the sender. The emails were also sent to large numbers of individuals with various ISPs, making it difficult for one ISP to track the sender of the emails.

5. Jennifer Clason.

Jennifer Clason started working for Defendant Schaffer in 1999 and was paid $ 2,500 per month. Her compensation eventually increased to $ 9,000 per month. Working under Schaffer's direction, Clason was the individual responsible for sending many of the emails at issue in this case.

Clason testified that Schaffer trained her in January of 2004 to send bulk pornographic emails. She used a computer at Schaffer's house. Schaffer showed her how to remotely access the servers in Amsterdam, set up the emails, and transmit the emails from the servers. Schaffer instructed her not to save anything to the computer, but instead to write her notes on paper.

Clason sent bulk emails for Defendants from April to October of 2004. She worked seven days per week, sending 10 to 12 batches of emails each day. The

evidence demonstrated that Schaffer sent the emails before April and after October of 2004.

At Schaffer's direction, [*25] Clason created approximately 200 domain names. She did so by combining two words to make nonsensical phrases such as "shoulderticks," "unthinkableflu," "salvationfling," and "carnagesupport." The domain names would then be registered to Ganymede (using Compston's credit card for TCC) and Clason would use them in the "from" line of the emails she sent, changing them frequently.

When sending an email from one of these domain names, Clason would make up a user name to place in front of the domain name. Thus, she might make up the user name "daniel" to combine with the domain name "shoulderticks," a combination which would then appear as "daniel@shoulderticks.com" in the email's "from" line. As explained above, Rogers' program would in turn take the recipient's user name and combine with it the domain name "shoulderticks" and place this combination in the header's return path.

Clason testified that she would place ambiguous phrases in the subject line of the emails such as "hi," "hello," or "hey you," and that she did this to make the emails look like they were being received from someone the recipient knew. Later, Clason began using more adult-oriented subject lines, but she never used "sexually [*26] explicit" in the subject line.

Clason testified that she initially sent an entire pornographic image with each email. Because ISPs began banning such emails, she would slice up the image and send it in portions with the email. The recipient's computer would re-assemble the image so that it would appear in full when the recipient opened the email.

As will be discussed more fully below, Counts 4-7 charge that two particular images sent by Defendants are obscene. One is titled "Fist Action" and the other is titled "Ass Munchers." Clason testified that she sent these images repeatedly at Schaffer's direction. She estimated that each image was sent approximately two times per week over the course of five months, for an estimated 40 times per image. Each time the images were sent they were received by thousands if not millions of recipients, as will be explained below.

6. Eric Zeller.

Eric Zeller is an internal investigator for AOL. Zeller's job is to investigate spam emails containing offensive or pornographic material. In 2004, Zeller became aware of a large volume of pornographic emails being sent to AOL customers from what appeared to be a single source. Upon investigation, he found that [*27] the domain names in the "from" lines of these emails consisted of two words joined together, such as "shoulderticks." Ultimately, Zeller identified 298 different domain names consisting of such a combination of words. His investigation identified "knllc.net" as a common denominator in the emails' routing information.

Zeller testified that AOL received 54,260 complaints about Defendants' emails on February 26, 2004 alone. AOL received 73,241 on March 2, 2004 and 76,525 on March 9, 2004. Dkt. # 319-3 at 31-33. Between December of 2003 and June of 2004, AOL received more than 662,934 complaints from customers who had received pornographic emails from Defendants. Zeller also testified that AOL retained only three to five percent of all of the complaints it received. These numbers demonstrate that Defendants were sending pornographic emails to literally millions of email addresses.

As part of his investigation, Zeller did a "Who Is" lookup on some of the domain names. (As Richard Kaplan testified, a "Who Is" lookup can be performed on the Internet at no charge and will identify the registrant of domain names.) The lookup results stated that the domain names were registered by Ganymede, a [*28] company based in Mauritius. Harry Plimpton was shown as the Ganymede contact person. Zeller tried to contact Plimpton at the phone number shown, but the phone number did not work. He did a Google search for Harry Plimpton and Ganymede, but could not locate them.

Zeller concluded from his investigation that header information in the emails was false. He noted that the "from" address and return path addresses typically were not the same. The registrant information was not accurate; he could not find Harry Plimpton. Nor could he locate knllc.net in Amsterdam. Despite his training and investigation, Zeller was never able to determine who sent the emails. Ultimately, Zeller turned his research over to the Government for further investigation.

7. Conclusions.

The evidence recounted above clearly established that the emails in question were "initiated" by Defendants

Kilbride and Schaffer within the meaning of the CAN-SPAM Act. Defendants initiated the emails in two ways. First, before April and after October of 2004, Schaffer personally originated and transmitted the emails from a computer at his house, using the remotely-accessed network in Amsterdam. *15 U.S.C. § 7702(9)*. This was done with [*29] the knowledge and assistance of Kilbride and as part of Defendants' ongoing spam email business. Second, between April and October of 2004, Defendants "procured" the origination and transmission of emails by paying Jennifer Clason to send them from Schaffer's house, again using the Amsterdam network. *15 U.S.C. § 7702(12)*. [3]

> 3 Even if Ganymede could be viewed as a separate "initiator" of the emails - a view the Court cannot accept given the central role and control of Defendants and the fact that Ganymede was essentially their alter-ego - the CAN-SPAM Act makes clear that "more than one person may be considered to have initiated a message." *15 U.S.C. § 7702(9)*. Kilbride and Schaffer instigated, directed, and were the ultimate financial beneficiaries of the spam email operation. They certainly qualify as "initiators" under the statute.

Defendants intentionally concealed from the headers any information that would allow themselves, as initiators of the emails, to be identified. This was done in a number of ways. They had Jennifer Clason make up domain names which were then registered to a Mauritius company which had a bogus contact person and phone number. The email software enabled Clason [*30] frequently to change the domain names from which the emails were sent. When compiling the "from" information for the emails, Clason would make up the user name to be placed before the domain names. The user name was not that of any individual associated with Defendants or Ganymede. The program was designed by Rogers to show a different return path, created by taking the recipient's user name and placing it before the domain name Clason made up. Although the emails all contained routing information with the common denominator "knllc.net," this was shown as an entity sending the emails from The Netherlands. And as Ellifson testified, knllc.net was a Wisconsin corporation neither owned nor operated by Defendants.

The ability of email recipients, ISPs, and law enforcement agencies to identify Defendants as the initiators of the emails was clearly impaired. If a recipient was sophisticated enough to do a "Who Is" lookup on the domain name, he would find that the name was registered to a company in Mauritius. The contact person for the company would be the non-existent Harry Plimpton. Were the person motivated enough to conduct investigations of Ganymede in the country of Mauritius, he would [*31] find that the directors were Christopher Compston from the Isle of Man and Laval Law from Mauritius. Defendants' names would not appear. If he were diligent enough to identify the owner of Ganymede, he would find that it was LHT, a trust under the control of Christopher Compston. Investigation into the source of funds used to register the domain names would show that the Isle of Man credit card of TCC had been used. Investigation into the actual source of the emails would show that they came from Amsterdam. Were an investigator to go to Amsterdam to determine who was affiliated with the computers there, he would not find the names of Kilbride or Schaffer, as Defendants clearly instructed Ellifson not to place their names on the computers.

In summary, the deliberately-crafted header information - the bogus user name with the ever-changing domain name, the false return path, and the identity of knllc.net in Amsterdam - concealed Defendants' identities and impaired the ability of email recipients, ISPs, or law enforcement agencies to determine that Defendants were the initiators. Even a trained ISP investigator like Eric Zeller could not identify Defendants. The evidence clearly established [*32] violations of *§ 1037(a)(3)*.

What is more, the evidence made clear that the violations were done "knowingly" as required by the Act. Defendants moved their operation offshore in late 2003 precisely to evade the strictures of the CAN-SPAM Act. Defendants falsified documents to justify their transfer of funds through Cardpro to Ganymede. Defendants arranged for all of their employees to enter consulting agreements with TCC rather than show a direct link to Ganymede. Defendants posed as Laval Law and Chad Smith when communicating with the operators of pornographic websites. Defendant Kilbride was furious when he received a call from someone inquiring about Ganymede, noting that the call did not look good on his phone records. Defendant Kilbride spoke truthfully when he told his co-conspirators that they would "cover" their "tracks."

Defendants argue that the header information was not false because it accurately led to Ganymede, the true registrant of the domain names. But the technical accuracy of this one fact does not cure the numerous misleading components of Defendants' header information. The Act prohibits the altering or concealing of information that would lead to the initiators [*33] of the emails. Defendants were the initiators. Ganymede was a front, a shill, and Defendants intentionally designed the header information to impair the ability of recipients and others to identify Defendants.

Defendants also argue that the header information is not false simply because the emails were initiated in Amsterdam, noting that many email senders use remote servers. Were the Amsterdam location of the servers the only evidence against Defendants in this case, the Court would agree. As noted above, however, Defendants engaged in an elaborate scheme, with many false components, in an effort to hide their role as the initiators of the emails. The jury's verdict on Count 2 was fully consistent with the weight of the evidence and the requirements of *§ 1037(a)(3)*.

IV. COUNT 3 - VIOLATION OF CAN-SPAM ACT *§ 1037(a)(4)*.

*Section 1037(a)(4)*authorizes the prosecution of any individual who knowingly:

> registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or on-line user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination [*34] of such accounts or domain names[.]

18 U.S.C. § 1037(a)(4). For purposes of this case, the statute makes it a crime for any person to register domain names and then initiate the transmission of multiple emails using those names, if, in the process of registration, the person used information that materially falsified the identity of the actual registrant. As already noted, "registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of the recipient of the message," an ISP, or a law enforcement agency "to identify, locate, or respond to a person who initiated the electronic mail message[.]" *18 U.S.C. § 1037(d)(2)*.

Defendants' argument is three-step: (1) the statute requires a person knowingly to falsify "the identity of the actual registrant," (2) Ganymede was the "actual registrant" of the domain names used in this case, and (3) the "identity" of Ganymede was not falsified - Ganymede actually registered the names and its identity was apparent to anyone who did a "Who Is" lookup on those names. Defendants argue that falsification of other information unrelated to the identity of the actual registrant - such as the false contact [*35] person, Harry Plimpton - does not violate *§ 1037(a)(4)* because it does not concern the "identity of the actual registrant."

This argument requires the Court to address the meaning of "actual registrant" in *§ 1037(a)(4)*. The CAN-SPAM Act does not define this phrase and it is not addressed in the most relevant legislative history. *See* S. Rep. No. 108-102 (2003). In the absence of a Congressional definition, the Court must look to the "'ordinary and natural' meaning" of the words. *Leocal v. Ashcroft, 543 U.S. 1, 8-9, 125 S. Ct. 377, 160 L. Ed. 2d 271 (2004)* (quoting *Smith v. United States, 508 U.S. 223, 228, 113 S. Ct. 2050, 124 L. Ed. 2d 138 (1993)*). This was the jury's task too, as the instructions requested by the parties and given by the Court merely used the statutory phrase "actual registrant" without elaboration. *See* Dkt. ## 232 at 31, 241 at 36, 330 at Instructions 28-29.

Courts "follow the common practice of consulting dictionary definitions to clarify" the "ordinary meaning" of statutory language. *United States v. TRW Rifle 7.62X51mm Caliber, One Model 14 Serial 5930006, 447 F.3d 686, 689 (9th Cir. 2006)* (quotation omitted). The Oxford English Dictionary provides the obvious definition of "registrant" as "[o]ne who registers" and "who thereby gains [*36] a particular entitlement." OXFORD ENGLISH DICTIONARY (2d. ed. 1989). In the context of the CAN-SPAM Act, the word clearly refers to one who registers a domain name with a registrar and thereby gains the right to use the name in email and on the Internet.

But Congress did not limit *§ 1037(a)(4)* to "registrant." The statute refers to the "actual registrant," suggesting a more searching inquiry. Oxford notes that the word "actual," when used to modify a noun, acts as an "intensifier" and is "[p]laced before a noun to emphasize its exact or particular identity," to reflect "its authentic or

archetypical status; genuine, real, typical." *Id.* (Addition Series 1997). Thus, the natural meaning of the phrase "actual registrant" would be the "exact," "genuine," or "real" registrant.

Given the evidence in this case, the jury reasonably could have concluded that Defendants Kilbride and Schaffer were the actual registrants of the domain names used to send their emails. Schaffer asked Clason to make up the names by combining two words to make a nonsensical phrase. The goal was to develop several hundred domain names that could be rotated frequently in the sending of the pornographic emails. The names [*37] would then be used by Defendants in sending emails from Schaffer's Arizona home. Although Kilbride would register the names with Ganymede as the purported registrant, the names were never actually used in Mauritius or even known to Laval Law, the only person in Mauritius with any formal relationship to Ganymede. The names were used by Schaffer and Clason, in the computer room of Schaffer's house, to send millions of spam emails.

To the extent Defendants now attempt to stand behind the Ganymede facade and claim that Ganymede was the actual registrant, their own fraudulent structure defeats their argument. Schaffer and Clason, the creators and users of the domain names, were not affiliated with Ganymede under the structure Defendants created. Schaffer had no formal relationship with Ganymede and Clason worked for TCC. If the domain names truly belonged to Ganymede, Ganymede never authorized Schaffer and Clason to use them. The fraudulent structure Defendants created thus belies their argument that Ganymede was the actual registrant and user of the names. In truth, the persons who created, registered, used, and profited from the domain names were Defendants. They were the men behind the [*38] curtain, the *actual* registrants.

Defendants suggest that such an application of the CAN-SPAM Act is dangerous because many persons and entities register multiple domain names for a variety of legitimate purposes in the far-flung world of the Internet, and domain names often are used on the Internet from remote locations. This may be true, but there is more to a violation of *§ 1037(a)(4)* than the mere registration and use of multiple domain names. The law also requires that the names be registered using information that is altered or concealed in a manner that impairs the ability of recipients to identify, locate, or respond to a person who initiated the message. *18 U.S.C. § 1037(d)(2)*. In other words, there must be an element of fraud, a deliberate hiding of the identity of the person initiating the email. Such a requirement comports with the CAN-SPAM purpose of prohibiting spammers "from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages." S. Rep. No. 108-102, at 1 (2003). Whatever close questions might arise in other cases where the motives or business methods of the defendants could be viewed as legitimate, those [*39] close questions do not arise here. The evidence made clear that Defendants embarked on a calculated program to hide their identities, avoid the strictures of the CAN-SPAM Act, and continue making millions through unsolicited pornographic emails. The elements of *§ 1037(a)(4)* were clearly satisfied by the Government's proof.

Moreover, even if Ganymede is viewed as the "actual registrant" of the domain names, the Government proved a violation of *§ 1037(a)(4)*. As the evidence established at trial, registration is more than merely providing the name of the domain name registrant to the registrar. Registration requires the registrant to provide contact information precisely for the purpose of enabling others to learn who is using the domain name and sending emails. The identity of a contact person who can receive communications on behalf of the registrant can fairly be viewed as part of the "identity" of the registrant. Without it, the registration provides little helpful information concerning the registrant.

When Defendants registered domain names to Ganymede in this case, they provided a false contact name of Harry Plimpton. They provided a false telephone number. They used Compston's credit [*40] card for TCC. In other words, they altered or concealed the registration information for the ultimate purpose of hiding their identities as initiators of the emails. The jury's verdict on Count 3 was correct.

V. COUNTS 4-7 - THE OBSCENITY CHARGES.

Counts 4 and 5 of the Indictment charge Defendants with importation or transportation of obscene material in violation of *18 U.S.C. § 1462*. Count 4 relates to an image titled "Fist Action" that was transmitted in some of Defendants' emails. This image, which appeared on the screen when recipients would open Defendants' emails, graphically portrays various individuals inserting their

entire fists into the anuses of other individuals. Count 5 relates to an image titled "Ass Munchers." This image graphically portrays multiple acts of oral-anal sex.

The Court instructed the jury that the Government had to prove three elements to establish the crimes charged in Counts 4 and 5: (1) that Defendants knowingly used an interactive computer service to transport the images in interstate commerce, (2) that Defendants knew the sexually oriented content of the images, and (3) that the images were obscene. Dkt. # 330, Instructions 34, 38.

Counts 6 and 7 charge [*41] Defendants with the transportation of obscene material for sale or distribution in violation of *18 U.S.C. § 1465*. Count 6 related to the image titled Fist Action and Count 7 related to the image titled Ass Munchers. The Court instructed the jury that the Government had to prove four elements to establish these crimes: (1) that Defendants knowingly transported the image in question using a facility or means of interstate or foreign commerce, (2) that Defendants transported such material for the purpose of sale or distribution, (3) that Defendants knew the sexually oriented content of the material, and (4) that the material was obscene. *Id.*, Instructions 40-41.

Defendants' motion addresses only the final element of these crimes - whether the images were obscene. Defendants make three arguments the Court will address separately.

A. Testimony of Email Recipients.

Defendants attack the testimony of six individuals who received Defendants' emails and complained. These individuals - Suzanne Schoenrock, Leonard Federico, Carolyn Gannon, Christina Fuocco, Kimberly Greenwald, and Scott Gilbert - each testified that they received the Fist Action image in one of Defendants' emails. Defendants claim [*42] that the evidence at trial demonstrated that none of these witnesses received the Fist Action image, that the witnesses therefore lied on the witness stand, and that the evidence was therefore insufficient to support the obscenity convictions. The Court does not agree.

First, the premise of Defendants' argument is incorrect. Defendants assert that these individuals established the community standards necessary for the obscenity determination. In fact, none of these witnesses testified directly about community standards. Moreover, as the Court instructed the jury, community standards is a broader inquiry:

> [You] should make the [obscenity] decision in the light of contemporary standards that would be applied by the average adult person in the community, with an average and normal attitude toward - and interest in - sex. Contemporary community standards are set by what is in fact accepted in the community as a whole; that is to say by society at large, or people in general, and not merely by what the community tolerates nor by what some persons or groups of persons may believe the community as a whole ought to accept or refuse to accept. The decision should not be based on your personal [*43] beliefs or opinions, but on the standards accepted by the community as a whole. Thus, in deciding whether the first two tests of the obscenity analysis have been satisfied, you must decide whether the images would appeal predominantly to prurient interests and would depict sexual conduct in a patently offensive way when viewed by an average adult person in the community as a whole. Matter is patently offensive by contemporary community standards if it so exceeds the generally accepted limits of candor in the community as to be clearly offensive. The "community" you should consider in deciding these questions is not defined by a precise geographic area. You may consider evidence of standards existing in places outside of this particular district.
>
> The parties have presented evidence concerning contemporary community standards. You should consider the evidence presented, but you may also consider your own experience and judgment in determining contemporary community standards.

Dkt. # 330, Instruction No. 36.

Defendants thus err in arguing that the testimony of the six email recipients was the source to which the jury was directed for determining community standards. As the Court's instructions [*44] made clear, jurors were to consider all of the evidence and their own experience. This included evidence of comparable images sold at various locations in Arizona, as presented by Defendants.

Second, contrary to Defendants' argument, the evidence did not establish that the six recipients lied when they said they had received the Fist Action image. Defendants base this argument on the fact that none of the AOL complaints contain the identifiers for the Fist Action website. But as Eric Zeller testified, AOL retained only three to five percent of the complaints it received. Thus, it is entirely possible that the witnesses received the Fist Action image, forwarded it to AOL in a complaint, and the complaint was among the 95 to 97 percent not retained.

In addition, Defendants assert that the Fist Action image was not sent by Defendants until after June of 2004 when AOL had blocked all emails from Defendants. Jennifer Clason testified, however, that she began sending emails on behalf of Defendants in April of 2004 and sent the Fist Action image in bulk emails at least twice per week. Her testimony supports the recipients' receipt of the Fist Action image through their AOL accounts. Moreover, [*45] Defendant Schaffer was sending the emails before Clason's involvement and was the one who directed Clason to send the Fist Action image. Thus, it is likely that Defendant Schaffer sent the Fist Action image in emails before Clason took over in April of 2004.

Third, Defendants argued vigorously at trial that the six witnesses lied. The jury had a full opportunity to weigh the credibility of the witnesses and concluded, nonetheless, that Defendants were guilty of Counts 4 through 7. Consistent with its obligations under *Rule 33*, the Court has also considered the credibility of the six witnesses and finds their testimony credible.

Fourth and most importantly, the Government did not need to prove that the six witnesses received the emails in order for Defendants to be convicted of Counts 4 through 7. Defendants do not dispute that they transmitted the Fist Action and Ass Munchers images in interstate commerce, for sale, and with knowledge that they were sexually explicit. The only question at trial, therefore, was whether the images are obscene. The jurors reasonably could have found the images obscene even if they concluded that the six witnesses never received them.

B. Defendants' Target [*46] **Lists.**

Defendants assert that they intended to send pornographic emails only to subscribers of adult websites. The evidence does not support this argument. Kirk Rogers testified that he configured the email software, at Defendants' direction, to permit emails to be sent to individuals who had requested that they be deleted from Defendants' email lists. He testified that this was to be done regularly, on a 30-day basis. This testimony suggested that Defendants deliberately sent their emails to individuals who did not want to receive them.

Several of the six recipient witnesses testified that they have never subscribed to pornographic websites. They nonetheless received emails from Defendants, including emails containing the Fist Action image.

More importantly, however, the crimes charged in Counts 4 through 7 do not require that Defendants send their emails to unwilling recipients or people who have never subscribed to pornography. The Government was required to prove only that Defendants knowingly sent sexually explicit images in interstate commerce and for sale, and that the images were obscene. The obscenity determination was to be made applying contemporary community standards. The [*47] jury could have believed Defendants' claim that they targeted only people who subscribe to Internet pornography and found, nonetheless, that the images are obscene.

C. Comparable Images.

Defendants argue that the jury could not have found the Fist Action and Ass Munchers images obscene because virtually identical images were located at stores in Arizona. The fact that comparable images are available elsewhere does not mean, however, that the images in this case are not obscene. As the Supreme Court has explained: "the mere fact that materials similar to the [images] at issue here 'are for sale and purchased at book stores around the country does not make them witnesses of virtue.'" *Hamling v. United States, 418 U.S. 87, 126, 94 S. Ct. 2887, 41 L. Ed. 2d 590 (1974)* (quoting *United States v. Hamling, 481 F.2d 307, 320 (9th Cir. 1973))*. The "'availability of similar material by itself means nothing more than that other persons are engaged in

similar activities.'" *Id.*

VI. COUNT 8 - CONSPIRACY TO COMMIT MONEY LAUNDERING.

Count 8 of the Indictment charges Defendants with conspiring to commit money laundering. Specifically, the Government alleged that Defendants conspired to violate *18 U.S.C. § 1956(a)(2)(B)(i)*. As the Court [*48] instructed the jury, a person violates this provision if each of the following elements occurs: (1) the person transports money from the United States to another country or from another country to the United States, (2) the person knows that the money represents the proceeds of some form of illegal activity, in this case violation of the CAN-SPAM Act as alleged in Counts 2 and 3, (3) the person knows that the transportation of the money is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of proceeds from a specific unlawful activity, in this case the transportation and sale of obscene materials as alleged in Counts 4 through 7, and (4) the person takes a substantial step toward committing this crime. Dkt. # 330, Instruction 46. For Defendants to be found guilty of conspiracy to violate this statute, the Government had to prove that (1) beginning on or about January 1, 2004 and ending on or about January 24, 2005, there was an agreement between two or more persons to commit the money laundering offense, and (2) Defendants became members of the conspiracy knowing of at least one of its objectives and intending to help accomplish [*49] it. *Id.*, Instruction 47.

Defendants' motion argues that the Government failed to prove the crime of conspiracy. Specifically, Defendants contend that the Government never proved that they actually earned money from sending spam emails or that money was actually earned from sending the Fist Action or Ass Munchers images. Defendants are incorrect.

The Government placed in evidence numerous documents from the bank accounts of Ganymede. These documents reflect numerous checks received by Ganymede during 2004 from pornographic website affiliate programs. (Under affiliate programs, websites pay commissions to persons who direct customers their way.) Evidence from Defendants' computers demonstrated that this money was received by Ganymede as a direct result of the pornographic email practices described above.

The Government presented the testimony of Ralph Gay, a financial expert whose firm reviewed the accounts of Ganymede. Mr. Gay presented a summary of checks received by Ganymede from pornographic website affiliate programs in 2004 (Ex. 570), totaling $ 1,218,889. This money came from 11 different pornographic website affiliate programs, including Platinum Bucks, Make . . . Money, Nasty Dollars, [*50] Top Bucks, Dollar Machine, Cash Quest, Porn Dollars, Electra Cash, Hustler Cash, Dino Publishing, and Gorilla Traffic. Dkt. # 319-13 at 47. Mr. Gay then traced proceeds from Ganymede to various aspects of Defendants' business operation, including payments for the computer network in Amsterdam, transfers of funds to TCC to be paid to Ellifson, Rogers, and Clason, and transfers of funds to trusts of which Defendants were the beneficiaries. This flow of proceeds showed money traveling from affiliate programs in the United States to bank accounts in the country of Mauritius, and back to trusts and individuals in the United States.

The Government also proved that Defendants received money from sending the Fist Action and Ass Munchers emails. James Fotrell, an investigator with the Department of Justice, imaged the hard drives from the two Amsterdam work stations used remotely by Defendants Kilbride and Schaffer. These computers contained a variety of records showing Defendants' receipt of money from pornographic website affiliate programs. Moreover, the records reflected money received by Defendants for the Fist Action and Ass Munchers images.

This evidence demonstrated that Defendants did [*51] in fact receive substantial income during 2004 from violations of the CAN-SPAM Act, and that those proceeds were used to maintain a business designed to conceal Defendants' receipt of money from the obscene images charged in Counts 4 through 7. It must be noted, however, that the Government did not need to prove the actual receipt of such proceeds in order for Defendants to be convicted of conspiracy. The Government merely had to show that there was an agreement between two or more persons to commit the money laundering offense identified in *18 U.S.C. § 1956(a)(2)(B)(i)*, and that Defendants became members of the conspiracy knowing of at least one of its objectives and intending to help accomplish it. Dkt. # 330, Instruction 47. The bank records and testimony of Mr. Gay and Mr. Fotrell demonstrated that Defendants clearly conspired to

commit the money laundering offense. The jury's verdict on Count 8 was consistent with the substantial weight of the evidence.

VII. JUROR 16.

Given the length of this trial and the nature of some of the pornographic images that would be shown to the jury, the Court elected to seat 12 jurors and four alternates, for a total of 16 jurors. The 16th juror was [*52] seated on the front row of the jury box, nearest to the prosecution's counsel table. Materials on the table were five to ten feet from Juror 16's view.

On three occasions during the trial defense counsel expressed concern that Juror 16 was looking at materials on the prosecution's table. This allegedly occurred during trial. Juror 16 made no effort to move closer to the prosecutors' table, but was seen by defense counsel looking in that direction.

After the issue had been raised twice by defense counsel, the Court made a point of watching Juror 16 more closely. On one occasion the Court saw Juror 16 look in the direction of a prosecutor as she turned and handed a note to a witness. Following this incident and a third expression of concern by defense counsel, the Court elected to question Juror 16.

On June 22, 2007, Juror 16 was brought into the courtroom during a break, with all counsel and Defendants present. Other jurors were not present. The Court explained on the record that it had seen Juror 16 looking at the prosecutor's table and had become concerned about whether Juror 16 was reading or viewing materials on the table or the prosecution's computer screens. The Court asked Juror [*53] 16 directly if he had seen or read any materials on the table. Juror 16 responded that he could see the computer screens, but could not read them, nor could he read materials on the table. The Court then asked this direct question: "Have you read any materials that have been on the prosecutor's desk or on their computer during the course of the trial?" Juror 16 responded "No." He then stated that he could not read without his glasses. The Court asked further: "So you haven't been able to see that information?" Juror 16 responded: "Nothing at all, sir." Following a few additional questions and the excusal of Juror 16, the Court made several specific findings. First, the Court found from Juror 16's responses that he was not reading material on the prosecutor's table. Second, the Court noted that it had never seen anything to lead the Court to believe that Juror 16 could actually read the material. Third, the Court found that Juror 16 was candid and truthful in his answers. On the basis of these conclusions, the Court declined to excuse Juror 16. [4]

> 4 The questions and answers quoted in this order, as well as the Court's findings, have been taken from the Court's real-time transcript of [*54] June 22, 2007, and should be reflected in the final trial transcript.

Noting that Juror 16 ultimately became the jury foreperson, Defendants seek a new trial under *Rule 33* on the ground that he was biased by material seen on the counsel table. For several reasons, the Court concludes that a new trial is not warranted.

First, "[a] defendant bears the burden of showing that a juror was actually biased against him or her and that the district court abused its discretion or committed manifest error when it failed to excuse the juror[.]" *United States v. Hanley, 190 F.3d 1017, 1030 (9th Cir. 1999)*. Defendants have not carried this burden. They reiterate a concern expressed during trial, but the Court specifically investigated their concern and found no reason to conclude that Juror 16 was biased or should be excused.

Second, on the basis of the Court's observations during the trial and Juror 16's candid responses to the Court's questions, the Court again concludes that Juror 16 did not view materials on the prosecution's table, was not biased, and therefore need not have been excused. This finding specifically is based on the inquiry the Court conducted after the concerns about Juror 16 had [*55] been raised.

Third, counsel for the Government avowed that they were being careful to keep exhibits and documents face down on the table and to turn their laptop computer screens so that they could not be viewed by jurors. The Court had no basis for doubting this avowal from the Government. It provides an additional basis for finding that Juror 16 was not exposed to improper material.

Fourth, Defendants argue that Juror 16's responses to the Court's questions must be disregarded because Juror 16 said he needed glasses to read, defense counsel never saw him wearing glasses during the trial, and Juror 16 apparently had no problem reading material on the display monitor in front of him which, defense counsel

asserts, was the same distance away as the prosecutors' notes. This argument is incorrect on several fronts. Although Juror 16 did assert that he needs glasses to read, the Court recalls seeing him wear glasses during the trial on several occasions as he was looking at his notes and at the display monitor before him. The display monitor is mounted on the inside of the jury box, less than one foot from Juror 16's right knee. The Court saw Juror 16 lean forward from time to time for a [*56] closer look at the monitor, but never saw him lean forward to look at material on the prosecutors' table.

Fifth, in addition to making specific inquiry of Juror 16, the Court gave the following instruction to the jury at the close of the case: "In reaching your verdict, you may consider only the testimony and exhibits received into evidence." Dkt. # 330, Instruction 7.

Sixth, removal of Juror 16 was not required under applicable case law. As the Supreme Court has explained:

> [D]lle process does not require a new trial every time a juror has been placed in a potentially compromising situation. Were that the rule, few trials would be constitutionally acceptable. The safeguards of juror impartiality, such as *voir dire* and protective instructions from the trial judge, are not infallible; it is virtually impossible to shield jurors from every contact or influence that might theoretically affect their vote. Due process means a jury capable and willing to decide the case solely on the evidence before it, and a trial judge ever watchful to prevent prejudicial occurrences and to determine the effect of such occurrences when they happen. Such determinations may properly be made at a hearing like [*57] that ordered in *Remmer [v. United States, 347 U.S. 227, 74 S. Ct. 450, 98 L. Ed. 654, 1954-1 C.B. 146 (1954)]* and held in this case.

Smith v. Phillips, 455 U.S. 209, 217, 102 S. Ct. 940, 71 L. Ed. 2d 78 (1982).

In *Remmer*, the trial court was directed "to determine the circumstances, the impact thereof on the juror, and whether or not [they were] prejudicial, in a hearing with all interested parties permitted to participate." *347 U.S. at 230*. That is precisely what the Court did in this case.

IT IS ORDERED that Defendants' Motion for Judgment of Acquittal or, In The Alternative, a New Trial Pursuant to *Fed. R. Crim. P. 29* and *33* (Dkt. # 301) is **denied.**

DATED this 24th day of August, 2007.

David G. Campbell

United States District Judge