

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED

2007 JUN 13 AM 11:40

CLERK US DISTRICT COURT
WESTERN DISTRICT OF TEXAS

BY [Signature]
DEPUTY

STATE OF TEXAS,

Plaintiff

vs.

ALONZO VILLANUEVA

Defendant

§
§
§
§
§
§
§
§

A07CA465 SS
Civil Action No. _____

PLAINTIFF'S ORIGINAL COMPLAINT

TO THE HONORABLE UNITED STATES DISTRICT COURT JUDGE:

Plaintiff the STATE OF TEXAS, acting by and through the Attorney General of Texas, GREG ABBOTT, files this Original Complaint against Defendant ALONZO VILLANUEVA and for causes of action would respectfully show the Court as follows:

JURISDICTION AND VENUE

1. This action is brought by Attorney General Greg Abbott, through his Consumer Protection & Public Health Division, in the name of the STATE OF TEXAS and in the public interest under the authority granted to him pursuant to the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701 *et seq.* ("CAN-SPAM Act"), by the Texas Electronic Mail Solicitation Act, TEX. BUS. & COM. CODE § 46.001 *et seq.* (Vernon Supp. 2006), and by the Deceptive Trade Practices - Consumer Protection Act, TEX. BUS. & COM. CODE § 17.41 *et seq.* (Vernon 2002 & Supp.2006) ("DTPA").
2. The Court has jurisdiction over the subject matter of these claims pursuant to 28 U.S.C. §§ 1331 & 1337(a). The Court further has supplemental jurisdiction over the subject matter of

the state law causes of action pursuant to 28 U.S.C. § 1367(a).

3. Venue of this suit lies in the Western District of Texas, Austin Division pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims alleged herein occurred within the Western District of Texas, as more specifically described below.

DEFENDANTS

4. Defendant ALONZO VILLANUEVA A/K/A [REDACTED] is an individual who resides at 1318 Gardina, Allen, Collin County, Texas 75002.

“SPAM” AND THE FEDERAL CAN-SPAM ACT AND THE TEXAS ELECTRONIC MAIL SOLICITATION ACT

5. In passing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701, *et seq.*, known as the “Can-Spam Act,” Congress found that the “convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail” and estimated that in 2003 such unsolicited commercial electronic mail “accounted for over half of all electronic mail traffic, up from an estimated seven percent in 2001.”
6. Congress further found that “the growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment,” and that “the receipt of a large number of unwanted messages...decreases the convenience of electronic mail and creates a risk that wanted...messages...will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the

reliability and usefulness of electronic mail to the recipient.”

7. Congress specifically found that “many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail” and “purposefully include misleading information in the messages’ subject lines in order to induce the recipients to view the messages.”
8. In passing the Can-Spam Act, Congress did not declare the mere sending of unsolicited commercial e-mail unlawful, but rather addressed specific problems associated with the rapid growth and abuse of unsolicited commercial electronic mail. For example, Congress specifically declared it unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if the header information is misleading or the subject heading would be likely to mislead a recipient acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message. Congress further required that such messages include a valid physical address for the sender as well as a method for the consumer to request not to receive future messages.
9. The State of Texas has also acted to protect the public interest from problems associated with the abuse of unsolicited commercial electronic mail and enacted the Electronic Mail Solicitation Act which, like the federal CAN-SPAM Act, does not prohibit sending unsolicited commercial electronic mail, but rather addresses the manner in which the e-mail messages are sent and received.

PUBLIC INTEREST

10. Plaintiff, STATE OF TEXAS, has reason to believe that the Defendant has engaged in and will continue to engage in a pattern or practice of unlawful practices as set forth below.

Plaintiff has reason to believe that an interest of the residents of Texas has been, or is threatened or adversely affected by Defendant's practices as alleged herein. Plaintiff also has reason to believe that the Defendant has caused and will continue to cause immediate irreparable injury, loss, and damage to the STATE OF TEXAS, and will also cause adverse effects to legitimate business enterprises which lawfully conduct trade and commerce in this State.

ACTS OF AGENTS

11. Whenever it is alleged in this petition that the Defendant did any act, it is meant that the Defendant performed or participated in the act.

NATURE OF DEFENDANT'S OPERATION AND STATEMENT OF FACTS

A. "SPAM"

12. Defendant has been and, on information and belief, continues to be involved in sending unsolicited commercial electronic mail ("e-mail"), otherwise known as "spam," to consumers in Texas and throughout the United States. Defendant's e-mail messages advertise a variety of goods and services, including but not limited to software security products and herbal remedies. Plaintiff has reason to believe that in most cases Defendant does not actually sell the goods and services advertised. Instead, Defendant earns money as an "affiliate" to the individuals or companies that are selling the products or services. It is believed that the Defendant receives compensation based on the total number of e-mail recipients who view the advertised web sites or purchase the advertised goods.
13. The amount of spam sent by the Defendant is unknown to Plaintiff at this time, but based on information and belief, Plaintiff alleges that the Defendant has sent thousands of such e-mails

between April 14, 2004 and the present. For example, between April 14, 2004 and October 22, 2004, Defendant sent more than 1,861 commercial e-mails to MSN Hotmail "spam traps."¹ Of the batch of e-mails sent to Hotmail's spam traps, the overwhelming majority violate the CAN-SPAM Act because they contain misleading subject lines, are void of valid sender e-mail addresses, lack physical mailing addresses, and/or fail to clearly and conspicuously identify the messages as advertisements, as described more fully below.

14. Defendant uses a variety of misleading methods in the mass distribution of his e-mail solicitations. Specifically, Defendant's commercial e-mail messages contain false, misleading and deceptive information in the subject line or subject heading, including but not limited to the following:

- (a) His baby pics;
- (b) I just hacked a guy; and
- (c) Hey;
- (d) Abbott; and
- (e) Keys.

Although the subject lines create an impression to the contrary, Defendant's e-mail messages advertise either male sexual enhancement pills, or "TraceDestroyer," (a computer program marketed purportedly to protect Internet usage history).

15. In addition, the commercial e-mail solicitations contain erroneous "from" return e-mail

¹These spam traps are e-mail accounts owned and maintained by Microsoft. Microsoft examines the e-mails received by these accounts as one of the methods it uses to determine whether incoming mail complies with the Terms of Use and Anti-Spam Policy for its MSN and MSN Hotmail services. The identity of these accounts is confidential, and the account names must remain confidential, so that spammers cannot avoid detection by removing the accounts' e-mail addresses from their lists.

addresses. Defendant attempts to “personalize” the spam by including common names, in lieu of proper return e-mail addresses. For instance, many of Defendant’s e-mail messages read “From: ‘Marline,’ ‘Pearl,’ or ‘Terrence.’” Defendant’s use of these common names likely serves two purposes. First, the common name is an attempt to dupe recipients into believing that they may have possibly received a legitimate e-mail from an acquaintance. The technique is designed to play on a recipient’s skepticism, if not curiosity. Second, using a false name in lieu of the sender’s actual name or e-mail address obscures the sender’s true identity.

16. Although falsifying the subject lines and the recipient e-mail addresses are each independent violations of the CAN-SPAM Act and the Texas Electronic Mail Solicitation Act, both create even more consumer confusion taken in unison. In one instance, an e-mail sent from “Edward,” with no valid return e-mail address, carried the subject line: “Arnold” and included the following representations:

“Do you visit porno sites?
Have erotic chats with others online?
Are you having an affair with somebody?

What would happen if your wife/husband or girlfriend/boyfriend found out.
Would it ruin your relationship?

Stop others from seeing what you do online.

<http://www.aol.com/ams/clickThruRedirect.adp?551,499,http://wejsnsl.info/index.php?id=173&affid=6206>

ahpeqghdqdyhkdfutwjgiqimst²

²The random string of characters listed in the last line of the e-mail message is a method spammers use in an attempt to circumvent spam blocking programs. See William S. Yerazunis, PhD. *Sparse Binary Polynomial Hashing and the CRM114 Discriminator*, MITSUBISHI ELECTRIC RESEARCH LABORATORIES, Jan. 20, 2003 at http://crm114.sourceforge.net/CRM114_paper.html.

Clicking on the above listed link leads the recipient to a web site selling the "TraceDestroyer" software, where the recipient is encouraged to purchase the software product.

17. In another example, Defendant sent an e-mail message using the name, "oscar@chello.nl," subject line, "I just hacked a guy," and included the following representations:

"theres no doubt getting old affects our sexaul [sic] life, now there is a solutoin [sic] to help

longer erectoins [sic]
increased [sic] sperm production

better than vaigra

<http://rd.yahoo.com/ahalf/qiyhk/iqri/qplg/?http://www.safegrow.biz/index.php?id=29>

Again, the listed hyperlink directs the recipient to a web site selling herbal remedies.

18. In nearly all instances, the Defendant's e-mail messages fail to clearly and conspicuously disclose that they are commercial solicitations. In addition, many of the Defendant's e-mail messages do not include an Internet-based mechanism for recipient consumers to prevent future correspondence. Finally, none of the Defendant's e-mails carry a physical address. Each of the above is a direct violation of the CAN-SPAM Act.

Defendant Acted Knowingly in Violating the CAN-SPAM Act

19. Through the course of its investigation, Plaintiff discovered Internet web postings by Defendant on a web site tailored to individuals with a common interest in spamming. The web site serves as a forum where individuals and affiliates can offer services (many times

of the malicious type), locate people or entities interested in sending spam, or exchange ideas, among other things. Based on information and belief, Defendant is a member of several of these spamming Internet web sites and communicates under the Internet user name [REDACTED]

20. Through this open Internet forum, the Defendant has revealed that he has previously been sued for violations of the CAN-SPAM Act, and yet flagrantly continues to offer the same services. On March 7, 2005, using the Internet name [REDACTED] Defendant authored the following web posting apparently addressing other members' concerns about the Defendant's reputation and ability to continue to transact spamming business:

...and for those of you who are "scared"[] to talk to me because of the deal with microsoft you can stop worrying. Everybody in the mailing biz [spamming] over reacted over nothing. I settled with microsoft exactly 3 days after i got served. Its done, its over and gone. If your interested hit me up on icq. **And yes artis, this is a spam service.** You got a problem with it you go talk to preston gates and have him sue me again. Bill's daddy loves to sue! (Emphasis added).

Indeed, the Defendant is referencing a State of Washington case styled: Microsoft Corp. v. Pelo, Villanueva, et al, No. 04-2-12465-4 SEA (May 3, 2005). Yet, despite a previous injunction, Defendant is undeterred from continuing his spamming services as evidenced by his offerings.

21. This is not the only indication of Defendant's intentions. On June 23, 2005, one member of the spamming forum posted a question querying the kinds of spam other members were sending: "Is ADULT [pornography] the only industry you're in?" In response to the posting, Defendant replied: "For the past few months ive [sic] been doing nothing but mainstream,

casino, loans, mortgages, credit cards, auto insurance, dating, anti spyware/virus and “legal downloads,” (meaning the Defendant was sending spam associated with the listed “industries.”) Despite having been sued by Microsoft for violations of the CAN-SPAM Act, the Defendant flagrantly continues to disregard the law.

B. “BOTNETS”

22. In addition to the Defendant’s alleged spamming violations, Defendant has also engaged in more technical and malicious means of distributing spam by organizing and offering to sell what is commonly referred to as a “botnet.” A botnet is a group of compromised computers infected with a minute program which grants a user control and functionality via the Internet, in most cases without an owner’s knowledge or consent.³ The individual who controls the botnet is called the “controller” or “bot herder.” There are numerous methods for bot herders to round-up innocent third party computers connected to the Internet. For example, some unscrupulous bot herders will dedicate time and resources searching for and exploiting computers with commonly-known vulnerabilities via the Internet. Once a computer is found, there are several different ways to upload an inconspicuous program onto the target computer: like sending a deceptive e-mail message beckoning the receiver to open what is believed to be a legitimate program, or embedding a virus or Trojan horse in another program offered on an Internet web site. Once the target computers are infected the controller can then summon the compromised computers and remotely command them to begin sending out mass amounts of spam. (Once a computer is infected and enslaved, it is sometimes referred

³“A botnet, short for *robot network*, is an aggregation of computers compromised by bots that are connected to a central ‘controller.’” Botnets are the focal point for a host of different Internet schemes, in particular the distribution of spam. *Informational Whitepaper: Current Malware Threats and Mitigation Strategies*, US-COMPUTER EMERGENCY READINESS TEAM, (May 16, 2005).

to as a "zombie"). While the tiny software programs used to infect computers come in several different flavors (*i.e.* spyware, malware, Trojan horses, backdoors, etc.), they are all crafted for one common purpose – to allow a controller unauthorized, undetected access usually in furtherance of a computer related violation or crime.

23. The very nature of a botnet is malicious. Notwithstanding the trespass and the breach of computer security violations, spammers have taken great interest in using botnets for a number of reasons. First, a botnet gives spammers access to literally thousands of infected computers which can easily and simultaneously assist in the procurement of mass amounts of commercial e-mail messages. Second, using a botnet obscures the identity of the true controller. In the case of spamming, recipients receive e-mail from an otherwise random computer, leaving the true sender hidden upstream.

24. Based on information and belief through the course of Plaintiff's investigation, Defendant has engaged in offering, for compensation, the use of a botnet for the purpose of distributing spam and engaging in other illegal acts. On August 18, 2005, Defendant [REDACTED] posted the following offering on a known spamming Internet web site:

Multiple proxy slots + botnet installs

socks 4/5/https proxies
10k + connects
updated every 15 minutes
fresh network, low rbls.

Proxy lock slot: rbl free proxies, 10,000 every 5 minutes, socks 4, \$1300 per week.
Ip restricted at the bot. Bank wire or paypal only for this slot.
I also have rbls free botnet installs to offer. 100,000 us/ca/mx/eu installs available of any exe you wish. The price for installs is \$70 per thousand or \$5000 for the whole network. Bank wires only for amounts [sic]over \$2000. Everything else below that can be paid however you like. icq: 269087034

25. Based on information and belief from the posting, the Defendant has control of a botnet,

apparently consisting of approximately 100,000 infected Internet computers, and is offering access and control to the computers for a host of malicious possibilities, which includes allowing a purchaser to upload additional programs. The posted fee for his services is \$70 per thousand computers, or \$5,000 for the entire botnet.

26. As a follow-up posting to his initial offer, Defendant added the following later the same day:

80k installs still available. I can run your exe before you pay if you have 2 good references. All installs are exclusive so nobody else will have any exes running on your bots.

Again, the Defendant reaffirms his intentions of selling a compromised botnet. Here, it appears that between the time of the first posting and the second, Defendant successfully sold access for installs to approximately 20,000 infected computers.

FIRST CAUSE OF ACTION

VIOLATIONS OF THE CAN-SPAM ACT

27. Plaintiff realleges paragraphs one through twenty-six in this Complaint and incorporates them here as if set forth in full.

28. Defendant engaged in a pattern or practice of initiating, to protected computers, commercial e-mail messages that:

- a. contained header information that was materially false or materially misleading;
- b. contained subject headings that the Defendant knew, or reasonably should have known, were likely to mislead recipients, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the messages;
- c. failed to contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit

- a request not to receive future commercial electronic mail messages from the sender;
 - d. failed to include clear and conspicuous identification that the message was an advertisement or solicitation; and
 - e. failed to provide a valid physical postal address of the sender.
29. Defendants' conduct violated 15 U.S.C. §§ 7704(a)(1-3) and (5) of the CAN-SPAM Act.

SECOND CAUSE OF ACTION

VIOLATIONS OF THE TEXAS ELECTRONIC MAIL SOLICITATION ACT

30. Plaintiff realleges paragraphs one through twenty-six of this Complaint and incorporates them here as if set forth in full.
31. Defendant intentionally transmitted commercial electronic mail messages that:
- a. falsified the electronic mail transmission information; and
 - b. contained false, deceptive, or misleading information in the subject line.
32. Defendant's conduct violated §§ 46.002(a)(1-2) of the Texas Electronic Mail Solicitation Act which prohibits the intentional transmission of commercial electronic mail messages that contain false, misleading or deceptive information in the subject line.

THIRD CAUSE OF ACTION

VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

33. Plaintiff realleges paragraphs one through twenty-six and incorporates them herein as if set forth here in full.
34. Defendant utilized misleading subject lines, misleading sender e-mail addresses, deceptive messages, and failed to disclose a physical mailing address.
35. Defendant offered to sell a network of illegally compromised computers, otherwise known

as a "botnet," without proper consent, thereby representing that the offer involves rights that are prohibited by law.

36. Such false, misleading, or deceptive acts and practices are in violation of DTPA §§ 17.46(a), (b)(1-3), (5), (12), and (24).

PRAYER

37. Because the Defendant has engaged in the acts and practices described above, Defendant has violated the law as alleged in this Complaint and, unless restrained by this Honorable Court, Defendant will continue to violate the laws of the UNITED STATES OF AMERICA and the STATE OF TEXAS and will cause immediate and irreparable injury, loss, and damage to the STATE OF TEXAS and to the general public.

38. WHEREFORE, Plaintiff prays that the Court:

- a. award Plaintiff such preliminary and ancillary relief as may be necessary to prevent the likelihood of consumer injury during the pendency of this action, and
- b. permanently enjoin the Defendant from continuing to violate the CAN-SPAM Act, the Texas Electronic Mail Solicitation Act and the Texas Deceptive Trade Practices Act.

39. In addition, Plaintiff STATE OF TEXAS respectfully prays that this Court adjudge against Defendant civil penalties in favor of Plaintiff STATE OF TEXAS as follows:

- a. Two Hundred and Fifty and No/100 Dollars (\$250.00) for each violation of 15 U.S.C. § 7704(a)(1) of the CAN-SPAM Act.
- b. Two Hundred and Fifty and No/100 Dollars (\$250.00) for each violation of 15 U.S.C. § 7704(a)(2) of the CAN-SPAM Act.

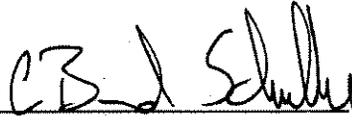
- c. Two Hundred and Fifty and No/100 Dollars (\$250.00) for each violation of 15 U.S.C. § 7704(a)(3) of the CAN-SPAM Act.
 - d. Two Hundred and Fifty and No/100 Dollars (\$250.00) for each violation of 15 U.S.C. § 7704(a)(5) of the CAN-SPAM Act.
 - e. Seven Hundred and Fifty and No/100 Dollars (\$750.00) each violation of 15 U.S.C. § 7704(a) of the CAN-SPAM Act that was committed willfully and knowingly.
 - f. Ten Dollars (\$10.00) for each unlawful message or action or Twenty-Five Thousand Dollars (\$25,000.00) for each day an unlawful message is received or an action was taken by Defendant in violation of § 46.002(a)(2) of the Texas Electronic Mail Solicitation Act; and
 - g. Twenty Thousand Dollars (\$20,000.00) for each violation of § 17.46(a) and (b) of the Texas Deceptive Trade Practices Act.
40. Plaintiff STATE OF TEXAS further prays that this Court order the Defendant to pay all costs of Court, costs of investigation, and reasonable attorneys' fees authorized pursuant to 15 U.S.C. § 7706(f)(4) of the CAN-SPAM Act and TEX. GOV'T CODE § 402.006(c) (Vernon Supp 2004-2005).
41. The Plaintiff further prays that the Court grant all other relief to which the Plaintiff may show itself entitled.

GREG ABBOTT
Attorney General of Texas

KENT C. SULLIVAN
First Assistant Attorney General

JEFF L. ROSE
Deputy First Assistant Attorney General

PAUL D. CARMONA
Chief, Consumer Protection and Public Health
Division



C. BRAD SCHUELKE
JOHN D. SABA JR.
Assistant Attorney General
Consumer Protection & Public Health Division
State Bar No.24008000
State Bar No.24037415
P. O. Box 12548
Austin, Texas 78711
(512) 463-2185
FAX (512) 473-8301