

1 Lawrence P. Riff (State Bar No. 104826)
lriff@steptoe.com
2 Lynn R. Levitan (State Bar No. 176737)
llevitan@steptoe.com
3 **STEPTOE & JOHNSON LLP**
633 West Fifth Street, Suite 700
4 Los Angeles, California 90071
Telephone: (213) 439-9400
5 Facsimile: (213) 439-9599

6 Attorneys for Plaintiff
HYPER TOUCH, INC.

7
8 **UNITED STATES DISTRICT COURT**
9 **CENTRAL DISTRICT OF CALIFORNIA**

10 HYPER TOUCH, INC., a California
11 corporation,

12 Plaintiff,

13 vs.

14 AZOOGLE.COM, INC., a Delaware
corporation d/b/a EPIC
15 ADVERTISING, INC.,
AZOOGLEADS USA, INC. a
16 Delaware corporation d/b/a EPIC
ADVERTISING, INC.; QUICKEN
17 LOANS, INC., a Michigan
corporation, SUBSCRIBERBASE,
18 INC., a South Carolina corporation
d/b/a ADDRIVE.COM, CONSUMER
19 RESEARCH CORPORATION, INC.,
FREE SLIDE, INC. AND
20 SUBSCRIBERBASE HOLDINGS,
INC., and DOES 6-10,

21 Defendants.
22

Case No. CV-08-03739 (GHK)
(PJW)

**FIRST AMENDED COMPLAINT
FOR DAMAGES AND
INJUNCTIVE RELIEF – Violation
of California Business &
Professions Code §§ 17529.5 and
17200 et seq., trespass to chattels**

DEMAND FOR JURY TRIAL

23 Plaintiff Hypertouch, Inc. (“Hypertouch”) brings this action seeking damages and
24 injunctive relief against Azoogle.com, Inc. d/b/a Epic Advertising, Inc., AzoogleAds USA,
25 Inc. d/b/a Epic Advertising, Inc. (collectively “Azoogle”), Quicken Loans, Inc., (“Quicken
26 Loans”), SubscriberBASE, Inc. d/b/a AdDrive.com, Consumer Research Corporation, Inc.,
27 Free Slide, Inc. and SubscriberBASE Holdings, Inc. (collectively, “SubscriberBASE”), and
28

1 Does 1-10 for violation of California Business & Professions Code §§ 17529.5 and 17200 *et*
2 *seq.*, and trespass to chattels, and alleges as follows:

3 1. Hypertouch is a California-based Internet Service Provider, or “ISP.”

4 2. As an ISP, Hypertouch receives and delivers thousands of e-mails each day to
5 its individual and business subscribers, as well as offering a variety of other services,
6 including the hosting of websites.

7 3. Hypertouch is an electronic mail service provider, which is an intermediary in
8 sending and receiving electronic mail and provides to end users of this electronic mail
9 service the ability to send or receive electronic mail.

10 4. Hypertouch® is a registered federal trademark (#2328650 and #2367595) for
11 computer services, first used in commerce in 1998.

12 5. Hypertouch owns and operates mail servers, web servers, and DNS (Domain
13 Name Service) servers that are connected to and accessed over the Internet.

14 6. In addition to legitimate e-mail, Hypertouch’s mail servers receive, each day,
15 thousands of unwanted and unsolicited commercial e-mails. Such unsolicited commercial
16 e-mail is known by various names, including “UCE” or “spam” and accounts for over 95%
17 of messages sent to Hypertouch’s mail servers.

18 7. Congress, in the Controlling the Assault of Non-Solicited Pornography and
19 Marketing Act of 2003 (the “CAN-SPAM” Act), moved to regulate unsolicited commercial
20 e-mail. While Congress legalized spam, it demanded transparency and accountability: thus,
21 federal law and the laws of 34 States, prohibit spam that contains false or misleading
22 information.

23 8. In CAN-SPAM, Congress made comprehensive legislative findings on the
24 burdens posed by spam (15 U.S.C. § 7701(a)):

25 a. “The convenience and efficiency of electronic mail are threatened by the
26 extremely rapid growth in the volume of unsolicited commercial
27 electronic mail. Unsolicited commercial electronic mail is currently
28 estimated to account for over half of all electronic mail traffic, up from

1 an estimated 7 percent in 2001, and the volume continues to rise. Most
2 of these messages are fraudulent or deceptive in one or more respects.”

- 3 b. “The receipt of unsolicited commercial electronic mail may result in
4 costs to recipients who cannot refuse to accept such mail and who incur
5 costs for the storage of such mail, or for the time spent accessing,
6 reviewing, and discarding such mail, or for both.”
- 7 c. “The receipt of a large number of unwanted messages also decreases the
8 convenience of electronic mail and creates a risk that wanted electronic
9 mail messages, both commercial and noncommercial, will be lost,
10 overlooked, or discarded amidst the larger volume of unwanted
11 messages, thus reducing the reliability and usefulness of electronic mail
12 to the recipient.”
- 13 d. “The growth in unsolicited commercial electronic mail imposes
14 significant monetary costs on providers of Internet access services,
15 businesses, and educational and nonprofit institutions that carry and
16 receive such mail, as there is a finite volume of mail that such providers,
17 businesses, and institutions can handle without further investment in
18 infrastructure.”
- 19 e. “Many senders of unsolicited commercial electronic mail purposefully
20 disguise the source of such mail.”
- 21 f. “Many senders of unsolicited commercial electronic mail purposefully
22 include misleading information in the messages’ subject lines in order to
23 induce the recipients to view the messages.”

24 9. Likewise, the California Legislature in enacting that state’s anti-spam law,
25 California Business & Professions Code §§ 17529 *et seq.*, found that (§ 17529(a)-(m)):

- 26 a. “Roughly 40 percent of all e-mail traffic in the United States is
27 comprised of unsolicited commercial e-mail advertisements (hereafter
28

1 spam) and industry experts predict that by the end of 2003 half of all e-
2 mail traffic will be comprised of spam.”

3 b. “The increase in spam is not only an annoyance but is also an increasing
4 drain on corporate budgets and possibly a threat to the continued
5 usefulness of the most successful tool of the computer age.”

6 c. “Complaints from irate business and home-computer users regarding
7 spam have skyrocketed, and polls have reported that 74 percent of
8 respondents favor making mass spamming illegal and only 12 percent
9 are opposed, and that 80 percent of respondents consider spam very
10 annoying.”

11 d. “According to Ferris Research Inc., a San Francisco consulting group,
12 spam will cost United States organizations more than ten billion dollars
13 (\$10,000,000,000) this year, including lost productivity and the
14 additional equipment, software, and manpower needed to combat the
15 problem. California is 12 percent of the United States population with
16 an emphasis on technology business, and it is therefore estimated that
17 spam costs California organizations well over 1.2 billion dollars
18 (\$1,200,000,000).”

19 e. “Like junk faxes, spam imposes a cost on users, using up valuable
20 storage space in e-mail inboxes, as well as costly computer band width,
21 and on networks and the computer servers that power them, and
22 discourages people from using e-mail.”

23 f. “Spam filters have not proven effective.”

24 g. “Like traditional paper “junk” mail, spam can be annoying and waste
25 time, but it also causes many additional problems because it is easy and
26 inexpensive to create, but difficult and costly to eliminate.”

27
28

- 1 h. “The “cost shifting” from deceptive spammers to Internet business and e-
2 mail users has been likened to sending junk mail with postage due or
3 making telemarketing calls to someone’s pay-per-minute cellular phone.”
- 4 i. “Many spammers have become so adept at masking their tracks that they
5 are rarely found, and are so technologically sophisticated that they can
6 adjust their systems to counter special filters and other barriers against
7 spam and can even electronically commandeer unprotected computers,
8 turning them into spam-launching weapons of mass production.”
- 9 j. “There is a need to regulate the advertisers who use spam, as well as the
10 actual spammers, because the actual spammers can be difficult to track
11 down due to some return addresses that show up on the display as
12 “unknown” and many others being obvious fakes and they are often
13 located offshore.”
- 14 k. “The true beneficiaries of spam are the advertisers who benefit from the
15 marketing derived from the advertisements.”
- 16 l. “In addition, spam is responsible for virus proliferation that can cause
17 tremendous damage both to individual computers and to business
18 systems.”
- 19 m. “Because of the above problems, it is necessary that spam be prohibited .
20 . . .”

21 10. In an April 2003 report entitled, *False Claims in Spam*, “the Federal Trade
22 Commission (FTC) found that 66 percent of all spam contains some kind of false,
23 fraudulent, or misleading information, either in the e-mail’s routing information, its subject
24 line, or the body of its message.” S. Rep. No. 108-102 (“CAN-SPAM Act of 2003”), at 2.
25 The FTC found that “one-third of all spam contains a fraudulent return e-mail address that is
26 included in the routing information (known as the ‘header’) of the e-mail message.” *Id.* at 3.
27 In the Senate Report, Congress also found that falsified headers “not only trick ISP’s
28 increasingly sophisticated filters,” but “lure consumers into mistakenly opening messages

1 from what appears to be people they know.” *Id.* In addition, Congress found that senders
2 use false or misleading subject lines to “trick the recipient into thinking that the e-mail
3 sender has a personal or business relationship with the recipient.” *Id.* at 4.

4 **PARTIES AND JURISDICTION**

5 11. Plaintiff Hypertouch is a California corporation, with its principal place of
6 business in Menlo Park, California. Hypertouch is developing next generation haptic
7 peripherals. None of Hypertouch’s peripherals that are in development have been released
8 to market and so are currently protected trade secrets. Hypertouch also provides Internet
9 services and consulting.

10 12. On information and belief, Defendant Azoogle.com, Inc. doing business as
11 Epic Advertising, Inc., is a Delaware corporation with its principal place of business in New
12 York, NY. Hypertouch is further informed and believes that Defendant Azoogle.com, Inc.
13 conducts business in, and under the laws of, the State of California.

14 13. On information and belief, Defendant AzoogleAds USA, Inc., doing business
15 as Epic Advertising, Inc., is a Delaware corporation with its principal place of business in
16 New York, NY. Hypertouch is further informed and believes that Defendant AzoogleAds
17 USA, Inc. conducts business in, and under the laws of, the State of California. Defendant
18 AzoogleAds USA, Inc. is a subsidiary of Azoogle.com, Inc.

19 14. On information and belief, Defendant Quicken Loans is a Michigan
20 corporation with its principal place of business in Livonia, MI. Hypertouch is further
21 informed and believes that Defendant Quicken Loans conducts business in, and under the
22 laws of, the State of California.

23 15. On information and belief, former Does 1-5, Defendant SubscriberBASE, Inc.,
24 doing business as AdDrive.com, Consumer Research Corporation, Inc., Free Slide, Inc. and
25 SubscriberBASE Holdings, Inc. (collectively, “SubscriberBASE”), are South Carolina
26 corporations with their principal place of business in Columbia, South Carolina.
27 Hypertouch is further informed and believes that Defendant SubscriberBASE conducts
28 business in, and under the laws of, the State of California.

1 16. Does 6-10 are persons to be identified. Plaintiff is unaware of the true names
2 and capacities of these defendants and therefore sues by such fictitious names. Plaintiff will
3 amend this complaint to allege their true names and capacities once ascertained.
4 Hypertouch is informed and believes and therefore alleges that each of the fictitiously-
5 named defendants is responsible in some manner for the occurrences herein alleged, and
6 that Hypertouch's injuries as herein alleged were proximately caused by such defendants.
7 These fictitiously-named defendants, along with Azoogle, Quicken Loans and
8 SubscriberBASE are herein referred to collectively as "Defendants."

9 17. Plaintiff is informed and believes that Defendants conspired to commit the acts
10 described herein, or alternatively, aided and abetted others in the performance of the
11 wrongful acts hereinafter alleged. All Defendants (including Does 6-10) agreed to,
12 authorized, participated in, acquiesced to, consented to and/or were the agents of another
13 defendant in the acts alleged, and initiated, conspired, assisted, participated in, or otherwise
14 encouraged the conduct alleged in furtherance of one or more conspiracies to send,
15 advertise in and/or initiate the e-mails. The transmissions of the e-mails identified herein
16 were actions that each of the Defendants authorized, controlled, directed, or had the ability
17 to authorize, control or direct, and were actions for which each of the Defendants is liable.

18 **ALLEGATIONS COMMON TO ALL CAUSES OF ACTION**

19 18. Hypertouch is an "electronic mail service provider" as defined in California
20 Business & Professions Code § 17529.1(h). Hypertouch provides and enables access to the
21 Internet for multiple users.

22 19. Hypertouch owns and operates interactive computer services that enable its
23 customers to, among other things, access the Internet, access Hypertouch-hosted Internet
24 services and exchange e-mail. Hypertouch owns and maintains computers and other
25 equipment, including specialized computers or "servers" that process e-mail messages and
26 otherwise support its e-mail services. Hypertouch maintains the e-mail-related equipment in
27 the County of San Mateo, California.

1 20. Each of Hypertouch's servers provides one or more services that enable users
2 to access content over the Internet. Hypertouch's clients could not access their e-mail
3 without Hypertouch's services. No user anywhere on the Internet can send e-mail to
4 Hypertouch's clients nor view the web pages of Hypertouch's clients without accessing the
5 servers provided by Hypertouch and using the services those servers provide.

6 21. All e-mail messages relevant to this litigation were sent to e-mail addresses
7 ordinarily accessed from computers located in this state.

8 22. Spam is by far Hypertouch's biggest customer service issue. Hypertouch has
9 suffered injury and lost money from its high spam load that includes the Defendants' spam.
10 This harm and cost includes, for example:

- 11 a. Decreased mail server and DNS server responsiveness;
- 12 b. Multiple mail server and DNS server crashes;
- 13 c. Mail server hardware and software replacements and upgrades to handle
14 the increased e-mail load;
- 15 d. Increased network bandwidth utilization;
- 16 e. Supplemental server, software and business broadband line purchases to
17 handle the increased e-mail load;
- 18 f. Delays in delivery of email from Hypertouch's servers and/or its clients
19 to other systems.

20 23. On information and belief, Defendants and/or their agents transmit and have
21 caused the transmission of commercial e-mail advertisements by bulk e-mail senders
22 ("spammers") from California and to e-mail addresses in California and other states.

23 24. On information and belief, Defendants and/or their agents also arrange and
24 have arranged with other companies to have commercial e-mail advertisements from
25 California and to e-mail addresses in California and other states.

26 25. On information and belief, Defendants and/or their agents advertised in, sent,
27 directed, assisted, encouraged, conspired in, procured, initiated, participated in and/or
28

1 facilitated the sending of tens or hundreds of thousands of e-mails to e-mail addresses both
2 in California and other states advertising various goods and services.

3 26. On information and belief, Defendants and/or their agents pay and have paid
4 others based on the number of people who “clicked-through” the links in those commercial
5 e-mail advertisements and thereby were directed to Defendants’ or a third-party advertiser’s
6 website and/or the number of people who made a purchase, participated in an “incentive”
7 program, submitted a mortgage lead or otherwise become a customer of the products or
8 services offered.

9 27. On information and belief, Defendants and/or their agents track and have
10 tracked the results of the transmissions and all related sales and services, in part so that the
11 bulk e-mailer whose e-mail lured the recipient to click through to the advertiser site could
12 be paid accordingly. This tracking generated records that identify the participants in these
13 activities, and the related times, dates, quantities and payment amounts.

14 28. On information and belief, Defendants and/or their agents advertised in
15 commercial e-mail advertisements sent via intermediary and/or third-party computers and
16 networks that were located in California to e-mail addresses both in California and other
17 states.

18 29. On information and belief, Defendants and/or their agents advertised in and
19 sent commercial e-mail advertisements to Hypertouch in California, and such e-mails
20 continue to arrive to this day.

21 30. On information and belief, Defendants and/or their agents agreed with and had
22 a meeting of the minds with each other and other third parties, including the Doe
23 defendants, to advertise in and send commercial e-mail advertisements received by
24 Hypertouch in California which contain or were accompanied by false or misleading
25 information.

26 31. On information and belief, Defendants and/or their agents acted to effectuate
27 their agreement, including by contracting with each other and other parties for the
28

1 advertising in commercial e-mail advertisements received by Hypertouch in California
2 which contain or were accompanied by false or misleading information.

3 32. On information and belief, Quicken Loans and Azoogole contracted for the
4 sending of commercial e-mail advertisements.

5 33. On information and belief, Quicken Loans and/or Azoogole contracted with
6 Does for the sending of commercial e-mail advertisements,

7 34. On information and belief, Defendants provided necessary assistance to the
8 spammers by paying them based on customer click-throughs.

9 35. On information and belief, Defendants benefited from the customer responses
10 generated by the spam.

11 36. On information and belief, Defendants were knowledgeable about the workings
12 of the internet marketing industry and the prevalent use of spam advertising in the industry.

13 37. Defendants' and/or their agents' conduct proximately caused harm to Plaintiff.

14 38. On information and belief, Defendants have engaged in unlawful, unfair or
15 fraudulent business acts or practices and unfair, deceptive, untrue or misleading advertising
16 and other acts prohibited by California law that proximately caused injury in fact and the
17 loss of money to Plaintiff.

18 39. Between April 15, 2004 and continuing to the present, Hypertouch received
19 over 380,000 e-mails attributable to Defendants. (Attached as Exhibits 1-11 are true and
20 correct sample copies of Defendants' e-mail received by Plaintiff.)

21 40. On information and belief, Plaintiff alleges Azoogole arranges and has arranged
22 with others to send spam to Plaintiff advertising its registered web properties, such as
23 SpicyMint, and on behalf of other advertisers.

24 41. On information and belief, Plaintiff alleges SubscriberBASE arranges and has
25 arranged with others to send spam to Plaintiff advertising its registered web properties, such
26 as HandbagTestPanel.com.

1 42. On information and belief, Plaintiff alleges the SubscriberBASE entities are
2 interrelated and function together in various roles in connection with the sending of and
3 advertising in e-mails.

4 43. On information and belief, Plaintiff alleges Quicken Loans arranges and has
5 arranged with others to send spam to Plaintiff advertising its mortgage loan business.

6 44. On information and belief, Plaintiff alleges Quicken Loans arranges and has
7 arranged with Azoogle to send spam to Plaintiff by or through Azoogle and other Doe
8 Defendants.

9 45. The e-mails received by Hypertouch contained or were accompanied by a third-
10 party's domain name without the permission of the third party.

11 46. The e-mails received by Hypertouch contained or were accompanied by
12 falsified, misrepresented and/or forged header information.

13 47. The e-mails received by Hypertouch had subject lines designed to and which
14 would be likely to mislead a recipient regarding the contents or subject matter of the
15 message.

16 48. On information and belief, Defendants and/or their agents also hired spammers
17 notorious for sending illegal spam to generate leads to which Defendants responded,
18 including by phone and e-mail. Generation of leads resulted in payments from Defendants
19 to ad networks and to spammers. Data contained in the e-mails allowed Defendants and/or
20 their agents to identify which ad networks and other collaborators in the spam e-mails were
21 responsible for generating the leads.

22 49. On information and belief, Plaintiff received commercial e-mail advertisements
23 sent by Defendants and/or their agents containing fraudulent, false, misrepresented and/or
24 forged header information. This includes, for example, that the e-mail arrived at the
25 Hypertouch servers containing or accompanied by false information concerning the
26 identities of the computers sending the e-mails.

27 50. When an e-mail arrives, the transmitting computer sends a "HELO," which is a
28 parameter typically showing the sending computer's name and/or IP address. This HELO

1 identifies the transmitting computer to the recipient computer in order to indicate where the
2 e-mail originated and/or was transmitted from.

3 51. With regard to the e-mails at issue, the identities of the transmitting computers
4 given in the HELO were falsified and did not match the IP addresses of the transmitting
5 computers. In other words, on information and belief, Defendants and/or their agents
6 falsified the identities of the transmitting computers by providing a HELO identifier that did
7 not match the actual IP address of the transmitting computer. This is done to prevent or
8 impair the identification of the actual sender of the spam and/or prevent or impair the
9 identification of the e-mail as unwanted spam.

10 52. Many of these e-mails are readily recognizable as belonging to Defendants
11 because the content in the e-mails advertises Azoogole-owned brands, such as
12 “ExtendedWarrantySavings.com” or “LowRateAdvisors.com”; because clicking on the link
13 in the e-mail leads to an Azoogole site, such as qckjmp.com/azjmp.com; because clicking on
14 the link in the e-mail leads to an SubscriberBASE site, such as HandbagTestPanel.com;
15 because the content in the e-mails advertises Quicken Loans-owned mortgages such as
16 “SmartChoice loan from Quicken Loans”; and/or because filing out a mortgage request form
17 results in Azoogole or one of its agents or Doe Defendants directing the lead to Quicken
18 Loans which then contacts the lead via e-mail and/or telephone.

19 53. For example in Exhibit 1, the sender used a computer at IP address
20 222.132.172.2, but that machine identified itself as “69.33.227.200,” which was actually
21 Hypertouch’s own mail server IP address. By using this blatantly false information the
22 senders of the mortgage spam made it appear as if Plaintiff was sending the e-mail.
23 Furthermore, the sender of the mortgage spam falsely claims to be “From:” Barksdale US
24 Air Force base in Louisiana, and to be sending the e-mail via a Cornell University mail
25 server, while using an IP address attributable in public records to a Chinese entity.

26 54. The multiple false elements Defendants used or condoned in Exhibit 1 in order
27 to generate leads for which Defendants paid spammers were designed to deceive the
28

1 recipient and mask the identity of the sender of the e-mails and to make it impossible to find
2 or contact the sender.

3 55. On information and belief, Plaintiff alleges that Azoogoo and/or other Doe
4 Defendants orchestrated the e-mail in Exhibit 1, among others at issue in this case, on behalf
5 of Quicken Loans. The spam advertised a mortgage inquiry webpage of www.b3mort.net.

6 56. On information and belief, test mortgage leads submitted to these websites
7 resulted in responses by Quicken Loans.

8 57. Mortgage spam is typically difficult to trace because it uses “throw-away”
9 domain names, such as falsely-registered domain names. Test mortgage leads are generated
10 from these e-mails accompanied by falsely-registered domain names. Thereafter, a
11 mortgage company responds after the lead has been submitted.

12 58. Defendant Quicken Loans responded to twenty-two different test leads
13 submitted by Hypertouch and other third parties to links advertised by spam e-mail
14 messages received by the Hypertouch’s mail servers. For example, Plaintiff received a
15 response e-mail from Quicken Loans with the subject line of “Subject: QuickenLoans has
16 received your Inquiry |” In the e-mail, Quicken Loans cited “MortgageRates4Less” as the
17 source of the loan request. Hypertouch is informed and believes that, at least seven months
18 prior to this contact, Quicken Loans was aware that MortgageRates4Less was generating
19 leads through illegal spam.

20 59. In another example, in Exhibit 2, Hypertouch’s mail server received a rejected
21 (“bounced”) spam from another ISP. In that e-mail advertising mortgages, the spammer
22 forged a hypertouch.com email address in the “From:” line. This false identification was
23 designed to deceive the recipient and mask the identity of the sender of the e-mails and to
24 make it impossible to find or contact the sender. The false From: line is also designed to
25 direct a bounce back not to the actual sender of the advertisement, but to an innocent third
26 party’s mail servers such as Hypertouch’s. The spam advertised a mortgage inquiry
27 webpage of www.b3mort.com.

28

1 60. Plaintiff alleges that Azoogle and/or other Doe Defendants orchestrated the e-
2 mail in Exhibit 2, among others at issue in this case, on behalf of Quicken Loans.

3 61. On information and belief, test mortgage leads submitted to these websites
4 resulted in responses by Quicken Loans.

5 62. In another example, in Exhibit 3, the sender used a computer at IP address
6 220.173.17.115, but that machine identified itself as “69.33.227.203,” which was actually
7 Hypertouch’s own mail server IP address. This false identification was designed to deceive
8 the recipient and mask the identity of the sender of the e-mails and to make it impossible to
9 find or contact the sender. The spam advertised a mortgage inquiry webpage of
10 www.wumort.net.

11 63. In Exhibit 3 the Date: line is also false.

12 64. Plaintiff alleges that Azoogle and/or other Doe Defendants orchestrated the e-
13 mail in Exhibit 3, among others at issue in this case, on behalf of Quicken Loans.

14 65. On information and belief, test mortgage leads submitted to these websites
15 resulted in responses by Quicken Loans.

16 66. In another example, in Exhibit 4, the sender falsified multiple lines in the e-
17 mail’s header to make it appear the e-mail was sent “From:” someone named “Geneva” at
18 Plaintiff’s company Hypertouch. No such employee or subscriber exists and thus the e-mail
19 header is false.

20 67. Among the header lines in Exhibit 4 is a falsified line purporting to show
21 receipt of the e-mail by the mail2.hypertouch.com server which is false because that line
22 was created by the spammer before they sent the e-mail to make it appear that the e-mail
23 was already accepted into Plaintiff’s system by Plaintiff’s firewall or spam filter. The spam
24 advertised a mortgage inquiry webpage of formsfresh.com.

25 68. Plaintiff alleges that Azoogle and/or other Doe Defendants orchestrated the e-
26 mail in Exhibit 4, among others at issue in this case, on behalf of Quicken Loans.

27 69. On information and belief, test mortgage leads submitted to these websites
28 resulted in responses by Quicken Loans.

1 70. Test mortgage leads generated for the purpose of identifying those responsible
2 for the spam by Hypertouch and, on information and belief, other recipients who completed
3 the mortgage application at the link provided in the e-mails led to domains including
4 www.b3mort.com and www.wumort.net (Exhibits 1-4), resulted in a direct response by
5 phone and/or e-mail from Quicken Loans.

6 71. For example, Plaintiff received an e-mail from Quicken Loans with the subject
7 line of “Subject: QuickenLoans has received your Inquiry |” In the e-mail, Quicken Loans
8 cited an entity called MortgageRates4less as the source of the loan request.

9 72. Hypertouch is informed and believes that at least seven months prior to this
10 contact from Quicken Loans, Quicken Loans was aware that MortgageRates4less was
11 generating leads through illegal spam.

12 73. In another example, Exhibit 5 shows an e-mail advertising a website owned by
13 Metareward. Clicking on the link in the e-mail caused the recipient to be directed to
14 Azoogles registered web property ackjmp.com, which then automatically redirects the
15 recipient on to Metarewards.

16 74. The sender of the e-mail in Exhibit 5 used a computer at IP address
17 204.13.20.2, but that machine identified itself as “mailpool.jriad.info,” which the spammer’s
18 own DNS server confirmed is a domain name having a different IP address. This false
19 identification was designed to deceive the recipient and mask the identity of the sender of
20 the e-mails and to make it more difficult, if not impossible, to find or contact the sender.

21 75. The domain name jriad.info used by the sender identified in paragraph 69 was
22 fraudulently registered using false and misleading owner information. This e-mail was sent
23 by the “Ralsky spam gang,” located in West Bloomfield, MI, based on information revealed
24 in discovery submitted by Azoogles to the court in another spam case this year in Santa Clara
25 county, 2-07-SC-004388.

26 76. At the time, Alan Ralsky was widely acknowledged as the most notorious
27 spammer in the world, for years ranked in the number one position of the Spamhaus
28 Project’s “Registry of Known Spam Operations.” The members of the Ralsky spam gang

1 were indicted by the Department of Justice on January 3, 2008. Statement of the
2 Department of Justice, *Alan Ralsky, Ten Others, Indicted in International Illegal Spamming*
3 *and Stock Fraud Scheme*, available at
4 <http://www.usdoj.gov/criminal/cybercrime/ralskyIndict.htm>. The 41-count indictment for
5 “a wide-ranging international fraud scheme involving the illegal use of bulk commercial e-
6 mailing, or ‘spamming’” was announced in a statement from the Department of Justice
7 which stated: “The flood of illegal spam continues to wreak havoc on the online
8 marketplace and has become a global criminal enterprise. It clogs consumers’ e-mail boxes
9 with scams and unwanted messages and imposes significant costs on our society. This
10 indictment reflects the commitment of the Department of Justice to prosecuting these
11 spamming organizations wherever they may operate.”

12 77. On information and belief, the notorious behavior of the Ralsky gang was well
13 known over the last five years to companies involved in the e-mail marketing field.

14 78. In another example, in Exhibit 6, the sender used computers at IP address
15 72.11.147.58, which identified itself fraudulently and falsely as “endogenter.com,” which is
16 itself a falsely-registered domain name.

17 79. The e-mail in Exhibit 6 fraudulently advertises ringtones at “No Charge” using
18 images hosted on Azoogles’ registered website at <http://i.1100i.com/>.

19 80. On November 7, 2007, the Attorney General of Florida announced a settlement
20 with Azoogles for a \$1,000,000 fine stemming from an investigation into the marketing of
21 ringtones and other cell phone products, on information and belief, similar to the advertising
22 in the e-mail in Exhibit 6. “Investigators determined that consumers, usually children or
23 teenagers who were responding to ‘free’ cell phone ringtone offers, were often enrolled into
24 subscription plans without their knowledge or consent.” See
25 [http://myfloridalegal.com/_852562220065EE67.nsf/0/86244EECC07CD59C8525738C00](http://myfloridalegal.com/_852562220065EE67.nsf/0/86244EECC07CD59C8525738C005DCDDF?Open&Highlight=0,azoogleads)
26 [5DCDDF?Open&Highlight=0,azoogleads](http://myfloridalegal.com/_852562220065EE67.nsf/0/86244EECC07CD59C8525738C005DCDDF?Open&Highlight=0,azoogleads).

1 81. In another example, in Exhibit 7, the sender used computers at IP address
2 72.11.146.11 and that computer fraudulently and falsely identified itself as “cgwcorps.com,”
3 which was a falsely-registered domain name.

4 82. The e-mail in Exhibit 7 shows Azoogle advertising its web property SpicyMint,
5 using images hosted on Azoogle’s website at <http://i.1100i.com/>.

6 83. In Exhibit 8, on information and belief, the sender fraudulently and falsely used
7 the domain “rit.edu” in the “From:” line in the e-mail’s header.

8 84. This false identification in Exhibit 8 was designed to deceive the recipient and
9 mask the identity of the sender of the e-mails and to make it impossible to find or contact
10 the sender.

11 85. The e-mail in Exhibit 8 advertised a mortgage inquiry webpage of
12 hreeonefiverose.com which generated leads which, on information and belief, Quicken
13 responded to.

14 86. In Exhibit 9, the sender used computers at IP address 72.11.144.10, and that
15 computer fraudulently and falsely identified itself as “gnbconnect.com,” which was a
16 falsely-registered domain name.

17 87. The e-mail in Exhibit 9 advertises Defendant Azoogle’s web property
18 LowRateAdvisors.

19 88. On May 5, 2008 Defendant Quicken Loans filed suit against Defendant
20 Azoogle.com, Inc and AzoogleAds.com Inc. for breach of Warranty, Breach of Contract and
21 Breach of Indemnity in connection with a previous anti-spam lawsuit by another ISP. In its
22 complaint, Defendant Quicken Loans included a copy of its contract with AzoogleAds.com,
23 Inc. specifying Azoogle’s LowRateAdvisors website, among other Azoogle properties (*See*
24 *Exhibit 13*).

25 89. The e-mail in Exhibit 9 advertising LowRateAdvisors uses images hosted on
26 Azoogle’s website at
27 http://i.1100i.com/2116/Nov2005/mailers/2/images/720x300_677_1.gif. In this e-mail, the
28 path name indicates that per Quicken Loan’s contract, Azoogle is purposely advertising its

1 property via electronic mail (i.e., “/Nov2005/mailers/”). In other words, this advertisement
2 was specifically created to be part of an electronic message mailing campaign.

3 90. Exhibit 10 contains a fraudulent, false and misleading “Free” From and Subject
4 line: i.e., “From: Handbag on us” and “Subject: -Get a free Handbag- choose from top
5 designers!”

6 91. On information and belief, the “free” Handbags from HandBagTestPanel.com
7 requires minimum purchases of over \$3,500.

8 92. The click-through link in the spam in Exhibit 10 advertising the “free”
9 handbags goes to Azoogole’s registered website <http://x.azjmp.com> which then automatically
10 redirects to HandBagTestPanel.com.

11 93. The owner of HandBagTestPanel.com, SubscriberBASE, recently settled with
12 the Washington State Attorney General over allegations of “deceptive practices in
13 marketing its online promotions.”

14 94. In addition, the sending domain name was falsely registered via
15 WhoisGuard.com, whose terms prohibit its domains from being used in spam, for the
16 purposes of concealing the true identity of the sender.

17 95. In Exhibit 11, the e-mail specifically advertises Quicken Loans as illustrated by
18 the subject line of the e-mail which advertises “Only \$688/Month for \$150,000!
19 SmartChoice loan from Quicken Loans.”

20 96. The Quicken Loans advertisement in Exhibit 11 used false third-party domain
21 names in the header.

22 97. The domain used in the body of the e-mail in Exhibit 11 is narzmort.com which
23 is listed with Spamhaus as belonging to Leo Kuvayev, “a spin-off or occasional partner with
24 Alan Ralsky.”

25 98. Upon information and belief, the 2005 websites used in Exhibits 1, 2, and 3
26 were all owned by Alex Polyakov. Defendant Quicken Loans responded to test leads
27 submitted for this spam run.
28

1 99. According to Spamhaus, “This spam operation [run by Polyakov] is large and
2 uses only hijacked-virus-infected-PC botnets to spam out of. Due to the number of fresh
3 machines they have access too, they are probably one of the larger virus/trojan creators and
4 spreaders.” This statement is consistent with Hypertouch’s observations of the Quicken
5 Loans mortgage spam its servers have received.

6 100. Upon information and belief, the 2006 websites used in Exhibit 4 are also
7 owned by Alex Polyakov. Defendant Quicken Loans responded to test leads submitted for
8 this spam run.

9 101. Upon information and belief, the 2007 websites used for example in Exhibit 8
10 are also owned by Alex Polyakov. Defendant Quicken Loans responded to test leads
11 submitted for this spam run.

12 102. Upon information and belief, Defendant Quicken Loans has used Alex
13 Polyakov for at least three years, despite numerous complaints to Quicken Loans regarding
14 their spam.

15 103. More than 40,000 of the e-mails at issue in this case used fraudulent and false
16 “From:” lines purporting to be from Hypertouch e-mail addresses.

17 104. By Defendants and/or Defendants’ spammers sending fraudulent and false,
18 misleading, harmful and vexatious e-mail advertising, including especially e-mail
19 purporting to come from Plaintiff – such as email purporting to come from Plaintiff’s mail
20 server (¶¶ 53, 62) or spoofed to come from “@hypertouch.com.” Defendants have harmed
21 Plaintiff’s business good will by causing false and fraudulent e-mails that appear to come
22 from it – making Hypertouch appear to be a spammer. In addition, by using
23 hypertouch.com addresses associated with spam, Defendants have, on information and
24 belief, impaired Hypertouch from delivering out-bound email to other ISPs. In other words,
25 other ISPs flag this e-mail as spam and can block such e-mails sent by Hypertouch’s
26 customers, including personal and work related e-mail.

27 105. Plaintiff received commercial e-mail advertisements sent by Defendants and/or
28 their agents containing fraudulent, false, misrepresented and/or forged header information in

1 that the e-mails contained one or more fictitious, false and/or misleading names in the
2 “From:” lines of the message headers. Defendants and/or their agents attempted to mislead
3 recipients by using different fictitious people’s names in the “From:” lines of the message
4 headers. For example, on April 16, 2005, the Defendants and/or their agents sent over 100
5 messages each with a From: line using a different quoted name consisting of 6-11 random
6 characters such as “moreomega.”

7 106. Plaintiff received commercial e-mail advertisements sent by Defendants and/or
8 their agents containing fraudulent, false, misrepresented and/or forged header information in
9 that the senders used false domain names in the sender addresses. Different e-mails sent
10 with different domain names were designed by Defendants and/or their agents to mislead
11 the recipients of the messages, mask the identity of the true sender of the e-mail, and to
12 deceive recipients and spam filters into *not* blocking the messages. (*See Exhibits 1-11*).

13 107. The Federal Trade Commission in its December 2005 report to Congress,
14 identified sending e-mails with many domain names and IP addresses as a deceptive means
15 of avoiding ISPs’ spam filters. *See Effectiveness and Enforcement of the CAN-SPAM Act: A*
16 *Federal Trade Commission Report to Congress*, at A-3 & n.74 (December 2005). By using
17 multiple domain names and IP addresses, Defendants were able to disguise the actual source
18 of the e-mail, and to trick ISPs by “spreading out” the total volume of e-mail, thus reducing
19 the volume sent from *each* domain name and IP address, and thus preventing spam filters
20 which react to large volumes of e-mail from a single source.

21 108. Plaintiff received commercial e-mail advertisements sent by Defendants and/or
22 their agents containing fraudulent, false, misrepresented and/or forged header information in
23 that the e-mails included domain names which were registered to false, non-existent entities,
24 as well as entities using false addresses and/or false telephone numbers. For example one
25 particular spammer of the Defendants employed over three thousand different domain
26 names using fake names, addresses and/or proxy services in the registration record (the
27 “Whois data”) for those domains to conceal the identity of the owner.

1 109. Plaintiff received commercial e-mail advertisements sent by Defendants and/or
2 their agents containing a reply address that was not and/or could not be functional because
3 the return address was connected with an invalid domain name or non-working account.
4 (*See, e.g.*, Exhibit 1.)

5 110. On information and belief, Plaintiff received commercial e-mail advertisements
6 sent by Defendant Azoogle, SubscriberBASE and/or its agents which intentionally
7 misrepresented, deceived, or concealed a material fact known to Azoogle and/or its agents
8 with the intention of depriving a person of property or legal rights or otherwise causing
9 injury.

10 111. On information and belief, Azoogle, SubscriberBASE and/or their agents sent
11 e-mails containing fraudulent and intentionally deceptive information in the subject lines
12 including, for example, stating that the e-mail recipient had won a “Free” gift such as a
13 “Complementary Plasma TV” or “-Get a free Handbag- choose from top designers!”
14 although in order potentially to receive any “free” item, the unknowing recipient had to sign
15 up for multiple sponsoring offers, and incur costs and obligations. *See* Exhibits 5, 10. The
16 subject lines were fraudulent and intentionally deceptive, and were designed, supplied,
17 approved or condoned by Azoogle, SubscriberBASE and/or its agents to deceive or attempt
18 to deceive the end recipient in order to cause the person to open the e-mail and undertake
19 obligations or pay money in order to receive items specifically advertised as “free,” a “gift”
20 or “complimentary.” The subject lines were fraudulent and intentionally deceptive, and
21 were designed, supplied, approved or condoned by Azoogle, SubscriberBASE and/or its
22 agents to cause the person to open the e-mail and undertake obligations or pay money in
23 order to receive a benefit, but the benefit was different than the one advertised to induce the
24 person.

25 112. On information and belief, Defendants and/or their agents sent e-mails with
26 subject lines that were also false because they contained characteristics that were designed
27 to deceive and evade receiving ISP’s spam filters and those of recipients. For example,
28 subject lines included deliberate misspellings, e.g. “Low mortgagge ratee approvall” in order

1 to deceive the end recipient, the receiving ISP and/or their spam filters, and were likely to
2 mislead a recipient.

3 113. E-mail with purposeful misspelling such as in ¶ 111 is sent as such for only one
4 purpose and that is to evade and deceive ISP and personal filters which key on certain
5 words in order to prevent unwanted e-mail – such as mortgage e-mail – from getting
6 through.

7 114. Although the federal CAN-SPAM Act requires all commercial e-mail to have
8 an opt-out mechanism, neither it, nor California law, make it a requirement for end users to
9 opt-out. To the contrary, major ISPs such as Microsoft, Earthlink, AT&T, Yahoo, Comcast,
10 Verizon, Charter, NetZero, and Qwest, warn against attempting to “opt out” of spam
11 because providing one’s e-mail address to spammers often subjects the recipient to more e-
12 mail. (*See* Exhibit 12.) Indeed, for example, some of the spam attributable to Ralsky
13 (Exhibit 5) was sent to e-mail addresses submitted to the opt-out links of other spam.
14 Hypertouch also warns its own users against attempting to “opt out” of spam they had not
15 requested in the first place.

16 115. Attempting to use Azoogle’s own opt-out mechanism directly to request that it
17 cease sending e-mail was ineffective and in fact subjected Plaintiff to new, additional spam
18 as Plaintiff’s e-mail address was given to other spammers. A unique e-mail address was
19 submitted to Azoogle’s opt-out mechanism. In just over two months, more than 1,000 new
20 spam were sent to that email address – an address never before nor since used anywhere
21 else.

22 116. These e-mails have harmed and continue to harm Hypertouch by interfering
23 with Hypertouch’s business operations, requiring the application of time, money and
24 technological resources to handle the spam. Among the adverse affects to Hypertouch that
25 high spam loads have caused are decreased server response and crashes, higher bandwidth
26 utilization, forced upgrades of expensive hardware and software, frustration of subscribers,
27 loss of business good will, delay of email delivery and loss of staff time. To the extent
28 Defendants’ thousands of e-mails consume disk space, create multiple files per email in disk

1 structure, drain the processing power of Hypertouch's computer equipment, and stress
2 Hypertouch's network infrastructure, those resources are not available to serve subscribers
3 or perform other tasks. Spam is Hypertouch's subscribers' number one complaint.

4 **FIRST CAUSE OF ACTION FOR VIOLATION OF**
5 **CALIFORNIA BUSINESS & PROFESSIONS CODE § 17529.5**

6 **(Against All Defendants)**

7 117. Plaintiff hereby repeats and re-alleges paragraphs 1 through 116 set forth above
8 as if fully set forth herein.

9 118. Under California Business & Professions Code § 17529.5(a), it is "unlawful for
10 any person or entity to advertise in a commercial e-mail advertisement either sent from
11 California or sent to a California electronic mail address" where that e-mail advertisement
12 "contains or is accompanied by a third-party's domain name without the permission of the
13 third party," "contains or is accompanied by falsified, misrepresented, or forged header
14 information," or "has a subject line that a person knows would be likely to mislead a
15 recipient, acting reasonably under the circumstances, about a material fact regarding the
16 contents or subject matter of the message."

17 119. Defendants and/or their agents sent and advertised in commercial e-mail
18 advertisements sent from California and received by Hypertouch in California at e-mail
19 addresses normally accessed from computers in the state.

20 120. Between at least April 15, 2004 and the present, inclusive, Defendants and/or
21 their agents advertised in, sent or caused to be sent at least 380,000 false and/or deceptive
22 commercial e-mail advertisements to Plaintiff's servers in violation of California Business
23 & Professions Code § 17529.5(a)(1), (2) and/or (3).

24 121. E-mail advertisements for or received from Defendants and/or their agents
25 contained or were accompanied by the fraudulent and false use of a third-party's domain
26 name without the permission of the third party and violate, for the reasons stated herein,
27 California Business & Professions Code § 17529.5(a)(1).

1 122. E-mail advertisements for or received from Defendants and/or their agents
2 contained and/or were accompanied by fraudulent, falsified, misrepresented, or forged
3 header information and violate, for the reasons stated herein, California Business &
4 Professions Code § 17529.5(a)(2).

5 123. E-mail advertisements for or received from Defendants and/or their agents
6 contained subject lines that a person knows would be likely to mislead a recipient, acting
7 reasonably under the circumstances, about a material fact regarding the contents or subject
8 matter of the message. For the reasons stated herein, these e-mails violated California
9 Business & Professions Code § 17529.5(a)(3).

10 124. Defendants conspired with each other and with others to send the unlawful
11 commercial e-mail advertisements. Defendants agreed to send e-mail advertising and took
12 actions to effect that result including but not limited to developing the e-mails, distributing
13 for use in the e-mails content and specifications, determining the recipients, paying others
14 for leads generated by the spam, contracting with each other to gain the benefit of the
15 advertising, and overseeing the use of Defendants' registered properties and brands in
16 connection with the spam.

17 125. Each e-mail is a separate violation.

18 126. Because of Defendants' repeated use of and contracting with spammers that
19 generated complaints and violation of their own policies and procedures by failure to
20 terminate known spammers, Defendants are liable for the full amount of statutory damages
21 permissible.

22 127. As a proximate result of the unlawful actions of Defendants and/or their agents,
23 Plaintiff suffered damages and is entitled to damages under California Business &
24 Professions Code § 17529.5(b)(1)(B) of \$1,000 per e-mail, Hypertouch's actual damages,
25 and its attorneys' fees.
26
27
28

1 D. Awarding Hypertouch damages for Defendants' intentional trespass on
2 Hypertouch's property;

3 E. Damages for civil conspiracy for the unlawful sending of commercial e-mail
4 advertisements;

5 F. Punitive damages against Defendant Azoogle and Defendant SubscriberBASE
6 under California Civil Code § 3294;

7 G. Enjoining temporarily and permanently Defendants, their officers, agents,
8 representatives, servants, employees, attorneys, successors, assignees, and all others in
9 active concert or participation with Defendants, from advertising in, initiating, conspiring,
10 or assisting in the sending of false or misleading commercial e-mail to Plaintiff under
11 California Business & Professions Code §§ 17203, 17204 and the inherent equitable powers
12 of this court; and

13 H. Awarding such other relief as this Court considers just and proper.

14
15 Dated: July 3, 2008

16 Respectfully submitted,
17 STEPTOE & JOHNSON LLP

18
19 By: 
20 Lawrence P. Riff
21 Lynn R. Levitan
22 STEPTOE & JOHNSON LLP
23 633 W. 5th St., Suite 700
24 Los Angeles, CA 90071
25 Tel: (213) 439-9400
26 Fax: (213) 439-9599

27 Attorneys for Plaintiff HYPERTOUCHE, INC.
28

JURY DEMAND

Plaintiff Hypertouch demands a trial by jury.

STEPTOE & JOHNSON LLP

By 
Lawrence P. Riff
Lynn R. Levitan
STEPTOE & JOHNSON LLP
633 W. 5th St., Suite 700
Los Angeles, CA 90071
Tel: (213) 439-9400
Fax: (213) 439-9599

Attorneys for Plaintiff HYPERTOUCHE, INC.