Evan A. Schmutz (3860)
eschmutz@djplaw.com
Jordan K. Cameron (12051)
jcameron@djplaw.com
DURHAM JONES & PINEGAR, P.C.
3301 N Thanksgiving Way, Suite 400
Lehi, Utah 84043
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff XMission, L.C.

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company, Plaintiff, vs. CLICKBOOTH.COM, LLC. a Florida Corporation; DOES 1-40, Defendants.	**DECLARATION OF PETER L. ASHDOWN** Case No.: 2:15cv00420 DBP Magistrate Judge Dustin B. Pead

I, Peter L. Ashdown, being first duly sworn and having personal knowledge of the matters asserted herein, do hereby declare as follows:

1. I am the founder of XMission, L.C.

2. I am currently the Chief Technical Officer and President of XMission.

3. I founded XMission in 1993 as Utah's first Internet Service Provider ("ISP").

4. From its early days as a private, Utah ISP, to its current role as a global business Internet provider, XMission has expanded its technical offerings to include sophisticated cloud hosting, web hosting, e-mail service and hosting, collaboration tools, business VoIP phone

service, and high speed Internet connectivity solutions including optical Ethernet, copper and fiber.

5. Throughout its history, XMission has also worked with hundreds of Utah's nonprofit organizations by providing free web hosting services, and by sponsoring a variety of community-based events and facilities.

6. XMission is a widely known and well-recognized ISP in Utah.

7. In cooperation with Salt Lake City government, XMission provides free WiFi to the downtown Salt Lake City metropolitan area.

8. XMission currently has 38 employees.

9. XMission owns all the servers, routers, and switches on its network through which it hosts and provides its Internet access services for its customers.

10. XMission has an expansive network and infrastructure, which it has had to consistently update, upgrade and augment in order to combat ongoing SPAM problems.

11. XMission is the sole owner of all its hardware, and has complete and uninhibited access to, and sole physical control over, the hardware.

12. XMission provides Internet access services to both commercial and residential customers.

13. The e-mail accounts hosted and served by XMission include e-mail accounts owned by third-party customers of XMission, e-mail accounts owned by employees and/or customers of XMission's third-party customers, e-mail accounts owned by employees of XMission, and also e-mail accounts owned by XMission itself.

14. XMission's network consists of approximately 65,000 mail accounts with 12,400 billable entities.

15. Throughout its business history, XMission has expended well in excess of $3,000,000 in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased SPAM and related harm, SPAM filtering expenses, and employee time in dealing with problems caused by its receipt of SPAM generally.

16. XMission expends approximately $100,000 to $200,000 per year in dealing with SPAM related issues and associated employee time, exclusive of attorney fees.

17. XMission has two full-time employees whose primary responsibilities are to deal with SPAM related issues, including, adjusting filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches, and hardware issues caused by SPAM.

18. XMission also employs 15 other technicians who dedicate at least part of their time to dealing with the aforementioned SPAM issues.

19. XMission currently has 13 servers dedicated specifically to process SPAM. Those servers could be dedicated to providing XMisson's Internet access services if it were not for the SPAM. XMission has had more total spam-mitigation servers over its history.

20. I estimate that SPAM takes up 13% of all general technical support staff and 39% of mail administrative time.

21. Daily between 40% and 85% of the e-mail messages that XMission receives on its system are SPAM e-mails, of which the subject e-mails are a part. Historically we can estimate an average spam level of 60% of all e-mail hitting XMission systems.

22. This number would be significantly higher if not for all the precautions that XMission has taken, including subscribing to leading anti-spam services, including blacklists such as URIBL and Spamhaus, in addition to creating customized and proprietary filtering rules and e-mail server configurations, utilizing tools such as SpamAssassin.

23. For each e-mail at issue in the lawsuit, XMission had to expend man hours and work to identify the source, to examine the transmission information, to examine and analyze the header information, to take efforts to determine how and why the specific e-mails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the e-mails stop.

24. In summary, the harm XMission suffered, and continues to suffer, as result of the ongoing SPAM problem is manifested in: financial expense and burden significant to XMission; lost employee time; lost profitability; the necessity to purchase and dedicate equipment specifically to process SPAM that could otherwise be dedicated providing Internet access services; harm to reputation; harm to XMission's goodwill; and customer and e-mail recipient complaints.

25. In my capacity as Chief Technical Officer, I oversee XMission's analysis and maintenance of data related to XMission's receipt of e-mail transmissions.

26. When any e-mail arrives on XMission's servers, it is assigned a Control ID number in the ordinary course of business.

27. XMission uses this Control ID number to keep track of e-mails and for convenience in creating summaries of data.

28. Regarding commercial SPAM e-mail, the e-mails will arrive on XMission's servers with hyperlinks intended to direct the recipient of the e-mail to a specific website, commonly known as a landing page.

29. The landing page typically is a website from which the e-mail recipient can purchase the product or service advertised in the e-mail.

30. Sometimes SPAM e-mails will serve other purposes, such as tracking valid recipient e-mail addresses or wanting an email response, such as those in phishing scams.

31. The links included in the e-mails are commonly known in the industry as redirect links.

32. A redirect link is not a direct path to a specific landing page, but rather consists of a series of links used by marketers and e-mail publishers to track e-mails for a variety of purposes, including cost-per-click compensation, and marketing analytics, to name a few.

33. As of June 11, 2015, XMission had identified 105,966 SPAM e-mails received over a relatively short period of time that XMission associated with Clickbooth.

34. Each of the e-mails in question contains redirect links through which Clickbooth is identified as the responsible transmitting party. Specifically, the redirect links include trackers owned by Clickbooth, including: clickbooth.com and clickbooth.net.

35. As part of my job responsibility, I oversaw the development and implementation of a mechanism whereby customers can lodge complaints to XMission related to SPAM e-mails they receive.

36. The complaint process allows customers to manually flag e-mails as SPAM, and thereby lodge a complaint with XMission related to that e-mail. It also allows customers to flag

certain criteria that will flag future e-mails as SPAM when received by that customer and thereby lodge a complaint with XMission. The complaint process is initiated by a manual action of the recipient.

37. When XMission receives customer complaints about SPAM e-mails, we will analyze the e-mail data to see if we can identify the source of the SPAM e-mails.

38. In this case, we were able to group all Clickbooth e-mails together by the trackers that Clickbooth includes in the redirect links.

39. XMission has recorded and preserved all of the original redirect paths included in the original e-mails at issue in this lawsuit on its servers.

40. Exhibit 1 hereto, is a sampling of redirect links in the actual e-mails in question. The complete redirect report is 34,084 pages long. XMission can provide it upon request from the Clickbooth or the Court.

41. XMission's Terms of Service provide that "XMission may take action on [customers'] behalf to mitigate SPAM and [customers] grant to XMission the authority and right to opt-out and/or unsubscribe from receiving any and all SPAM e-mails, sent by any party to your e-mail address(es)." *See Terms of Service*, ¶ 24, included herewith as Exhibit 2.

42. Pursuant to its Terms of Service XMission attempts, through automated means and otherwise, to click on all available opt-out links whenever a SPAM e-mail arrives on its servers.

43. XMission has attempted to click on available unsubscribe links in each of the received Clickbooth e-mails, but such does not appear to have stopped commercial e-mails. From this exercise, XMission has concluded that the unsubscribe links do not permit the

recipient to simply click the link in order to opt-out or require that the recipient take additional steps in order to actually opt-out.

44. On June 12, 2015, XMission filed a Complaint against Clickbooth for violations of 15 U.S.C. § 7701 et seq., otherwise known as the CAN-SPAM Act. Each of the e-mails is a commercial message and contains commercial content.

45. Each of the e-mail in question was received by XMission on its e-mail servers in Utah.

46. Included herewith on a data DVD (Exhibit 3) is a sampling of approximately 15,800 of the e-mails in question. The total number of e-mails at issue comprises more than 30 gigabytes of data and would span at least 7 data DVDs. However, Clickbooth can download each of the e-mails from a secure link that XMission will provide upon request.

47. XMission has preserved each of the e-mails in its original form just as it was received by XMission. XMission has redacted the recipient email address from each e-mail provided herewith and available on the aforementioned link pursuant to our privacy policy. XMission can provide e-mails with the recipient e-mail addresses once a protective order is entered by the Court to protect the confidentiality of the information.

48. The Exhibits to this Declaration summarize the data and information contained in the original, preserved e-mails.

49. The Clickbooth e-mails that XMission has received through June 11, 2015, have resulted in 9,372 customer complaints.

50. As of the date of this Motion, the e-mails are continuing on a daily basis, and XMission continues to receive customer complaints associated with the e-mails.

51. In the two days preceding the filing of its Complaint against Clickbooth, XMission received, and accounted for, 1,882 Clickbooth e-mails and received 61 customer complaints related to those e-mails.

52. One of XMission's competitive advantages is that is has historically been able to offer Internet access and business hosting services with greatly reduced SPAM traffic.

53. However, in recent years, as the number of SPAM e-mails has increased, the number of e-mails that are bypassing XMission's SPAM filtering techniques has continued to grow.

54. These e-mails include the e-mails at issue in this lawsuit.

55. In addition to specific customer complaints related to the Clickbooth e-mails, XMission's reputation and competitive advantage has been harmed, and will continue to be harmed, because customers have taken notice of the growing number of SPAM e-mails reaching their inboxes, and have expressed dissatisfaction with XMission and doubt as to XMission's ability to offer a SPAM free service.

56. If the e-mailing is allowed to persist, it will result in possible loss of customers, and a significant, and likely irreparable, damage to XMission's reputation and competitive advantage in the market place.

57. XMission also analyzes the header information and other transmission data in the e-mails.

58. Approximately 962 of the e-mails received through June 11, 2015, contained header information that included inaccurate sender IP addresses. These are IP addresses that either do not belong to the identified sender domain, were not recognized by a legitimate Domain

Name Service as belonging to identified legitimate domain, and/or do not identify the actual source of the e-mail.

59. XMission identified this information by performing a reverse DNS lookup when the e-mails were received on XMission's servers, and logged the results in the ordinary course of business.

60. Exhibit 4 hereto is a summary of data which includes a list of e-mails, identified by Control ID number, that contain a false or inaccurate IP address in the header information. XMission maintains all of the e-mails and data used to create this summary on its servers.

61. Approximately 18,884 of the e-mails received through June 11, 2015, contained generic "from" names and originated from privacy-protected sender domains.

62. XMission identified this information by analyzing the "from" name designated by the transmitting party and by performing a WHOIS look-up in publicly available WHOIS database, to gather privacy information on the sender domain.

63. The WHOIS database is an online repository of information associated with registered domain names. It stores and publicly displays domain name information, such creation and expiration dates, the registrar of record, and its various contacts (registrant, billing, administrative, and technical).

64. The sender domain is the e-mail domain (e.g @example.com) that was identified as the e-mail domain from which the e-mail was sent.

65. Exhibit 5 hereto is a summary of data which includes a list of e-mails, identified by Control ID number, an identification of the generic "from" name, and an identification of the

privacy protected sender domain. XMission maintains all of the e-mails and data used to create this summary on its servers.

66. Approximately 416 e-mails received through June 11, 2015, included a “from” name that was deceptive in order to induce the recipient to open the e-mail message under a false pretense.

67. The “from” names include, as examples, “Refinance Approvals”, “Credit Alert”, “Approval Department”, “LoanApproval Notice”, “Loan Manager”, and “Score update”. Exhibit 6 hereto is a summary of data which includes a list of e-mails, identified by Control ID number, that contain a materially misleading “from” name intended to induce the recipient to open the e-mail under a false pretense. XMission maintains all of the e-mails and data used to create this summary on its servers.

68. Approximately 100,612 of the e-mails received through June 11, 2015, originated from sender domains registered with ICANN compliant domain registrars who maintain anti-spam policies, and these sender domains served no purpose other than to engage in activities that violate the anti-spam policies.

69. XMission gathered this information by identifying the domain registrar information for each sender domain in publicly available WHOIS databases.

70. Through its research, XMission has determined that e-mails were sent from sender domains registered with: 1&1 Internet AG; BigRock Solutions, Ltd.; DomainDiscover; DomainSite, Inc.; Dynadot, LLC; Gandi SAS; GoDaddy.com; Internet.bs Corp.; Name.com, Inc.; Namesilo, LLC; PDR Ltd. d/b/a PublicDomainRegistry.com; Register.com; and, Wild West Domains, LLC.

71. Each of these domain registrars maintains anti-spam policies.

72. Each of the anti-spam policies is available to the public online.

73. 1 &1 Internet AG's *General Terms & Conditions* is located online at http://www.1and1.com/Gtc?__lf=Static&linkOrigin=&linkId=ft.nav.tandc.

a. I accessed and downloaded the *General Terms & Conditions* from its website and include the relevant sections as Exhibit 7, hereto.

b. The *General Terms & Conditions* require registrants to "agree and warrant that [they] shall not use any form of mass unsolicited electronic mail solicitations . . . or any other form of 'spamming' . . . ." Section 8.14. Additionally the *General Terms & Conditions* further require that registrants "Agree and warrant that [they] shall not engage in any false, deceptive or fraudulent activities . . . ." Section 8.15.

74. BigRock Solutions, Ltd.'s *Domain Registrant Agreement* is located online at http://www.bigrock.com/legal/?requestfor=registraragreement&from=agree_page.

a. I accessed and downloaded the *Domain Registrant Agreement* from its website and include the relevant sections as Exhibit 8, hereto.

b. The *Domain Registrant Agreement* requires the registering party to agree that it will not use the services for: "sending unsolicited mass e-mails (i.e., to more than 10 individuals, generally referred to as spamming) which provokes complaints from any of the recipients; or engaging in spamming from any provider." Appx. A(2)(3); "(1) transmitting Unsolicited Commercial e-mail (UCE); (2) transmitting bulk e-mail . . . . Appx. A(2)(9)(1); "transmitting bulk e-mail" (Appx. A(2)(9)(2)).

75. TierraNet d/b/a DomainDiscover's *Universal Terms of Service Agreement* is located online at https://www.tierra.net/TOS_current/universal_terms.

a. I accessed and downloaded the *Universal Terms of Service Agreement* from its website and include the relevant sections as Exhibit 9, hereto.

b. The *Universal Terms of Service Agreement* states, "you shall not distribute, publish, or send: (1) any spam, including any unsolicited advertisements, solicitations, commercial email messages, informational announcements, or promotional messages of any kind; (2) chain mail; (3) numerous copies of the same or substantially similar messages; (4) empty messages; (5) messages that contain no substantive content; (6) very large messages or files that disrupt a server, account, newsgroup, or chat service; (7) any message that is categorized as "phishing"; or (8) any other similar message or activity." *Universal Terms of Service Agreement*. Appx. A, Electronic Communications.

76. DomainSite, Inc. d/b/a Spot Domains's *Domain Name Registration Agreement* is located online at https://www.domainsite.com/policies/registration-agreement.php.

a. I accessed and downloaded the *Domain Name Registration Agreement* from its website and include the relevant sections as Exhibit 10, hereto.

b. The *Domain Name Registration Agreement* prohibits "the transmission of unsolicited email . . . ." Section 6.a.

77. Dynadot, LLC's *Service Agreement* is located online at https://www.dynadot.com/registration_agreement.html.

a. I accessed and downloaded the *Service Agreement* from its website and include the relevant sections as Exhibit 11, hereto.

b. The *Service Agreement* prohibits "[m]orally objectionable activities include[ing] . . .the transmission of unsolicited mail or 'spam' . . . ." *Service Agreement*, Section 7; *see also* Section 10.

78. Gandi SAS's *General Terms and Conditions of Domain Name Registration* is located online at http://www.gandi.net/contracts/en/g1/pdf/.

a. I accessed and downloaded the *General Terms and Conditions of Domain Name Registration* from its website and include the relevant sections as Exhibit 12, hereto.

b. *General Terms and Conditions of Domain Name Registration* states "You will not, and will not let others, use Our services, directly or indirectly to send spam (unsolicited bulk email)." Section 10.

79. GoDaddy.com's *Domain Name Registration Agreement* is located online at https://www.godaddy.com/agreements/showdoc.aspx?pageid=REG_SA.

a. I accessed and downloaded the *Domain Name Registration Agreement* from its website and include the relevant sections as Exhibit 13, hereto.

b. The *Domain Name Registration Agreement* requires the registering party to agree that it will not use the services for "[t]he transmission of unsolicited email." *See* Section 8.

80. Internet.bs Corp.'s *Terms and Conditions* is located online at http://www.internetbs.net/legal/Internet.bs-RegistrationAgreement.pdf.

a. I accessed and downloaded the *Terms and Conditions* from its website and include the relevant sections as Exhibit 14, hereto.

81. The *Terms and Conditions* state, "We reserve the right to immediately suspend, cancel, terminate, transfer or modify your Registration for any reason, including, without limitation, if: (i) your material breach of this Agreement; (ii) your use of any Services, including, without limitation, the domain registered to you, that is in contradiction of applicable laws or customarily acceptable usage policies of the Internet, including, without limitation, sending unsolicited commercial advertisements (including, without limitation, spamming) . . . ." *Terms and Conditions*, Section 15.a.

82. Name.com, Inc.'s *Domain Name Registration Agreement* is located online at https://www.name.com/policies/registration-agreement.

a. I accessed and downloaded the *Domain Name Registration Agreement* from its website and include the relevant sections as Exhibit 15, hereto.

b. The *Domain Name Registration Agreement* prohibits "the transmission of unsolicited email . . . ." Section 6.a.

83. Namesilo, LLC's *General Terms and Conditions* is located online at https://www.namesilo.com/Support/General-Terms-and-Conditions.

a. I accessed and downloaded the *General Terms and Conditions* from its website and include the relevant section as Exhibit 16, hereto.

b. Its *General Terms and Conditions* prohibits the use of its service in "violation of any third party's rights or acceptable use policies, including but not limited to the transmission of unsolicited email." Section 5.a. The *General Terms and*

Conditions further identifies, as abusive, and "Domains and web sites involved in the transmission of unsolicited email." *Id*. at Section 5.a.v.

84. PDR Ltd. d/b/a PublicDomainRegistry.com's *Registrar-Registrant Agreement* is located online at http://publicdomainregistry.com/legal/.

a. I accessed and downloaded the *Registrar-Registrant Agreement* from its website and include the relevant sections as Exhibit 17, hereto.

b. The *Registrar-Registrant Agreement* prohibits "sending unsolicited mass e-mail (i.e., to more than 10 individuals, generally referred to as spamming)" (*Registrar-Registrant Agreement*, Appx. A.2(3)), "transmitting Unsolicited Commercial e-mail (UCE)" (Appx. A.2(9)(1)); "transmitting bulk e-mail" (Appx. A.2(9)(2)).

85. Register.com's *Master Services Agreement* is located online at http://www.register.com/policy/servicesagreement.rcmx.

a. I accessed and downloaded the *Master Services Agreement* from its website and include the relevant sections as Exhibit 18, hereto.

b. Its *Master Services Agreement* states that a "Customer is prohibited from transmitting unsolicited commercial email." *See* Section 14.

86. Wild West Domains, LLC's *Wild West Domain Name Registration Agreement* is located online at https://www.wildwestdomains.com/agreements/ShowDoc.aspx?pageid=reg_sa.

a. I accessed and downloaded the *Wild West Domain Name Registration Agreement* from its website and include the relevant sections as Exhibit 19, hereto.

b. The *Wild West Domain Name Registration Agreement* prohibits "[t]he transmission of unsolicited email (Spam)[.]" *See* Section 8.

87. XMission has examined the identified sender domains and determined that they do not appear to resolve to any legitimate website or have any legitimate function other than mass e-mail marketing. *See* Exhibit 20 hereto, which is a compilation of all of the connection data related to the sender domains in question.

88. In fact, each of the sender domains at issue was used to transmit SPAM e-mail messages to XMission.

89. Exhibit 21 hereto is a summary includes a list of e-mails, identified by Control ID number, that were transmitted from domains registered with domain registrars that maintain anti-spam policies, and which sender domains served no purpose other than to engage in activities that violate the anti-spam policies. XMission maintains all of the e-mails and data used to create this summary on its servers.

I declare under penalty of perjury of the laws of that State of Utah and the United States of American that the foregoing is true and correct to the best of my knowledge.

EXECUTED this 12th day of June, 2015.

/s/ Peter L. Ashdown
Peter L. Ashdown

(* I certify that I have the signed original of this document which is available for inspection during normal business hours by the Court or a party to this action.

*Declaration electronically signed, pursuant to U.C.A. § 46-4-201(4) and District Of Utah CM/ECF and E-filing)