

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEB 15 2011

JAMES N. HATTEN, Clerk
[Signature]
Deputy Clerk

GREGORY D. EVANS, LIGATT
SECURITY INTERNATIONAL,
INC., and SPOOFEM.COM USA
INC.,

Plaintiffs,

vs.

JOHN DOES 1-8,

Defendants.

§
§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO.

111-CV-0458

FILED UNDER SEAL

**VERIFIED COMPLAINT FOR INJUNCTIVE
RELIEF, DAMAGES AND DEMAND FOR JURY TRIAL**

TO THE HONORABLE JUDGE OF THIS COURT:

Plaintiffs Gregory D. Evans (Mr. Evans) LIGATT Security International, Inc. ("LIGATT Security") and Spoofer.com USA Inc. ("Spoofer") (collectively "Plaintiffs"), by and through their undersigned counsel, hereby bring this action against John Does 1-8 (collectively "Defendants") and, in support thereof, alleges and states as set forth herein. Plaintiffs allege the following facts upon actual knowledge with respect to information concerning themselves and their own acts and upon information and belief as to all other matters. Unless specifically stated otherwise, Plaintiffs information and belief is based on information

uncovered by Plaintiffs on the Internet or other public forums or statement and admissions made or published by Defendants at the very websites used or controlled by Defendants.

NATURE AND BASIS OF ACTION

1. Plaintiffs bring this action against Defendants pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et. seq.*, the Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-90, *et. seq.*, and other laws to recover legal and equitable relief for Defendants' unlawful conduct constituting, among other things, tortuous interference with contractual relations, business relations, and potential business relations, trespass to chattels and misappropriation of Plaintiff's trade secrets. To redress the harm that Defendants have caused to Plaintiffs, Plaintiffs seek temporary, preliminary, and permanent injunctive relief, as well as compensatory damages, punitive damages, costs, and reasonable attorneys' fees and any and all appropriate additional relief.

THE PARTIES AND JURISDICTION

2. Plaintiff Gregory D. Evans is a Georgia resident and Chief Executive Officer of LIGATT Security and Spoofem.

3. Plaintiff LIGATT Security is a California corporation that is duly licensed to conduct business in the State of Georgia. LIGATT Security's principal

place of business is located at 6991 Peachtree Industrial Boulevard, Norcross, Gwinnett County, Georgia.

4. Plaintiff Spoofem is an Oklahoma corporation that is duly licensed to conduct business in the State of Georgia. Spoofem's principal place of business is located at 6991 Peachtree Industrial Boulevard, Norcross, Gwinnett County, Georgia.

5. Both LIGATT Security and Spoofem are publically-traded companies.

6. Defendants are "unknown" individuals who reside in various states within the United States. Due to the structure and operation of the Internet, which allows users to post content anonymously, Defendants have been able to conceal their identity and whereabouts by creating and posting content on the Internet using aliases. The actual names and addresses of the individual Defendants will be substituted by way of amendment of this pleading as soon as the individual Defendants' names and addresses are discovered through further investigation and discovery.

7. Upon information and belief, John Doe 1 is an individual who, without authorization, accessed one or more of Plaintiffs' computers and online accounts and acquired, downloaded, misappropriated and used proprietary,

trade secret, confidential and commercially sensitive information belonging to Plaintiffs and disclosed that information to third-parties on the Internet as more fully described throughout this Complaint.

8. Upon information and belief, John Doe 2 is an individual that owns, operates, administers, uses or maintains one or more websites using the domain names <ligattleaks.com>, <ligattleaks.net>, <ligattleaks.org>, ccTLD domain name <ligattleaks.blogs.ru> (collectively the "Ligattleaks Homepage") and maintains and uses an account at the real-time information network provided at www.twitter.com under the alias "ligattleaks" (the "Ligattleaks Twitter Page"). Based on prior communications with John Doe 2, Plaintiffs believe that John Doe 2 owns, uses or controls the email account associated with the address ligattleaks@hushmail.com.

9. Upon information and belief, John Doe 3 is an individual that owns, operates, administers, uses or maintains the website located at www.pastebin.com. Based on information provided on www.pastebin.com, Plaintiffs believe that John Doe 3 owns, uses or controls the email account associated with the address pastebin@gmail.com.

10. Upon information and belief, John Doe 4 is an individual that owns, operates, administers, uses or maintains one or more user or posting accounts at the website located at www.pastebin.com.

11. Upon information and belief, John Doe 5 is an individual that owns, operates, administers, uses or maintains a website located www.attrition.org and uses an account at the real-time information network provided at www.twitter.com under the alias "attritionorg" (the "Attrition Twitter Page").

12. Upon information and belief, John Doe 6 is an individual that uses an account at the real-time information network provided at www.twitter.com under the alias "lucky225" (the "Lucky225 Twitter Page").

13. Upon information and belief, John Doe 7 is an individual that owns, operates, administers, uses or maintains the website located at www.thetechherald.com. Based on information provided at www.thetechherald.com, Plaintiffs believe that John Doe 7 uses or maintains a physical address located at 320 N Parker Avenue, Indianapolis, IN 46201

14. Upon information and belief, John Doe 8 is an individual who accessed, downloaded, reviewed or otherwise acquired The Confidential Information (to be later defined) at The Pastebin Location (to be later defined).

15. Upon information and belief, Defendants maintain and operate computers and Internet communication links, and engage in other conduct, that purposefully avails them of the privilege of conducting business in Georgia, and further have purposefully directed and aimed the acts complained of herein toward Georgia, and have utilized instrumentalities located in Georgia to carry out the acts complained of herein. In particular, Defendants gained unauthorized access (hacked) into computers located in Georgia, including specifically computers located in the Northern District of Georgia, and used said access to view and copy information and stored communications, and to assume control of various of Plaintiffs online accounts and shutdown Plaintiffs' e-commerce website, by which conduct Defendants caused harm to Plaintiffs and their customers. Defendants have undertaken the foregoing acts with knowledge that such acts would affect computers and users of computers located in Georgia, thereby injuring Plaintiffs and their customers in Georgia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

16. This action arises out of the Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030). Therefore, the Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331. Plaintiffs also

bring an action for state-law claims arising from the same case or controversy, so this Court has supplemental subject matter jurisdiction over those claims pursuant to 28 U.S.C. § 1367.

VENUE

17. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district because a substantial part of the events or omissions giving rise to Plaintiffs' claims, together with a substantial part of the property that is the subject of Plaintiffs' claims, are situated in this judicial district. Further, venue is proper in this judicial district under 28 U.S.C. § 1391(c) because the Defendants are subject to personal jurisdiction in this judicial district.

FACTS COMMON TO ALL COUNTS

Background

18. Mr. Gregory D. Evans ("Mr. Evans") is the President and Chief Executive Officer of LIGATT Security and Spoofem. Mr. Evans founded LIGATT Security in 2003 and Spoofem in 2006 as small closely-held companies and has since grown both companies into nationally-renowned, publically-traded companies. As LIGATT Security's and Spoofem's business and notoriety expanded, Mr. Evans' renown and reputation as a digital and network security expert also grew.

19. Through his work with LIGATT Security, Spoofem, and other related undertakings, Mr. Evans has come to be regarded as one of the foremost authorities in the country on issues of computer, network and information security, appearing as a security expert on and in a number of well-known international cable news channels and publications, including CNN, Fox News, Bloomberg and Time Magazine.

20. Apparently, Mr. Evans' successes as a newcomer and quick-riser in the information security market have caused some market actors some degree of resentment and angst. *See, e.g.*, Exhibit A hereto, a printout of a blog located at <http://mpictcenter.blogspot.com/2011/02/ethical-hacking-and-ligatt-security.html> ("A lot of security professionals have been resisting Evans' activities, including me."). At some point during 2010, two or more individuals in the information security market formed a network or association that aimed, among other things, to establish a concerted and coordinated effort to discredit, besmirch, oppose or otherwise undermine Mr. Evans and his successful businesses (the "Anonymous Association").

Hacking and Cracking

21. Many, if not all, of the individuals that formed the Anonymous Association considered themselves to be "hackers." Typically, "hacking" of

computer security systems and/or the “cracking” of user passwords in order to gain unauthorized access to and trespass upon the computer systems of a given website or network fall into a category of activity considered to be prohibited or improper. In this context, a “hacker” is someone who subverts computer security without authorization or who uses technology (usually a computer or the Internet) for vandalism (malicious destruction), credit card fraud, identity theft, intellectual property theft, or many other types of crime or underhanded activities. This can mean taking control of a remote computer through a network, or a process known as “software cracking.”

22. “Cracking” is an umbrella term that refers to the various surreptitious and/or nefarious processes and modalities through which a hacker obtains username and password information in order to gain unauthorized access to a computer system.

23. Cracking can be accomplished by means of so-called “brute force attacks” whereby the hacker repeatedly inputs numerous possible username and password combinations until a successful combination is found and the hacker gains access to the computer system. Cracking is also at times accomplished by hackers who are able to learn or guess the password of an authorized user.

Plaintiffs and Their Businesses

24. LIGATT Security steadily built a reputation as one of this Country's premier hi-tech security companies and is recognized as a leader in computer security and cyber-crime investigation. Publically traded, LIGATT Security offers a number of cutting-edge security products directly to its customers at its website, located at www.ligattsecurity.com, and through various third-party vendors. LIGATT Security's product and service line include a number of innovative products and services that include solutions for anti-hacker, anti-spam, anti-spyware, and anti-virus issues. LIGATT Security has become well-known in the information security industry for its products and services, including, by way of example, its Locate PC product.

25. Spoofem, a sister-company to LIGATT Security, is a publically-traded company that offers a variety of products to its consumers that primarily relate to "caller identification spoofing" technologies. Caller identification spoofing is a concept that permits an end-user placing a call on a telephone network to mask or alter one or more of the caller's identifying characteristics (e.g., the caller's telephone number) that may be provided to the receiving party during the call or immediately prior to a connection being established.

26. At their websites, maintained at www.ligattsecurity.com and www.spoofem.com respectively, LIGATT Security and Spoofem: offer goods and services for sale; transact online product purchases; provide marketing and other informational materials about their products and companies; and provide a link that directs users to a location where end users can purchase public shares of each respective company. Plaintiffs maintain a web server at their business location that hosts their business websites. Plaintiffs also maintain at their business location a centralized server that houses company confidential and proprietary business information and private information (the "Service Management Server").

27. As part of its efforts to maintain an online presence and increase brand interest and loyalty, LIGATT Security uses and maintains an account with the online service provider operating at www.twitter.com. At all times relevant to this Complaint, LIGATT Security's Twitter account was password protected and LIGATT Security's practice permitted restricted access to the company's Twitter account.

28. At all times relevant to this Complaint, both LIGATT Security and Spoofem maintain confidential, private, proprietary and commercially sensitive information on one or more computers residing on their private business

network. Likewise, one or more computers on Plaintiffs' networks contained private information, including social security numbers and other personal information of Mr. Evans, Plaintiffs' customers, Plaintiffs' vendors and Plaintiffs' employees.

29. Both LIGATT Security and Spoofem take a number of steps to maintain the secrecy and private nature of their own confidential and proprietary business information and the personal information to which they are entrusted, including the use of secure networks, password-protected files, networks and databases, data encryption and other in-house technological security innovations. Plaintiffs also use a system and process to protect the confidential, private and proprietary in its ownership and control that incorporate a series of company security protocols, including the use of door codes, limited access to designated physical and virtual locations, limited handling of designated materials and other similar restrictions.

Defendants and Their Misconduct

30. On or about February 2, 2011, John Doe 1 accessed Plaintiffs' private business network by means of hacking or cracking (hereinafter, collectively referred to as "hacked" or "hacking").

31. On or about February 2, 2011, John Doe 1 accessed one or more computers on Plaintiffs' private business network by means of hacking, including Plaintiffs' internal Service Management Server and their web server. After hacking into Plaintiffs' network, John Doe 1 downloaded, copied or otherwise acquired confidential, proprietary, and commercially sensitive information from the Service Management Server, including at least passwords and pass codes to various virtual and physical company locations that housed additional confidential information. John Doe 1 further downloaded, copied or otherwise acquired the company's web files stored on Plaintiffs' web server and subsequently deleted those files from their location on Plaintiffs' web server. As a result, Plaintiffs' company websites were unavailable from the time of the hacking on February 2, 2011 until on or about February 8, 2011.

32. On or about February 2, 2011, John Doe 1 accessed Mr. Evans' company email account by means of hacking, and downloaded, copied or otherwise acquired in excess of 80,000 company emails, attachments included, stored in Mr. Evans company email account. The emails contained in Mr. Evans' account dated back at least 5 years and contained countless attachments and communications discussing and disclosing proprietary, confidential, commercially sensitive and private information.

33. On or about February 2, 2011, John Doe 1 accessed LIGATT Security's Twitter account and took control over the account, changing the account's user name and password. After assuming control of the account, John Doe 1 issued several statements from LIGATT Security's Twitter account, impersonating Mr. Evans and providing a link to the url <http://pastebin.com/raw.php?i=3k8jrMJn> (the "Pastebin Location").

34. After downloading, copying or otherwise acquiring the aforementioned files, data and information belonging to Plaintiffs ("The Confidential Information"), John Doe 1 posted or otherwise made available The Confidential Information at the Pastebin Location. In so doing, John Doe 1 did not redact the Confidential Information, use a simple search-and replace function, or otherwise remove individuals' Social Security numbers or bank account and routing numbers that were included in The Confidential Information. *See Exhibit A.*

35. The Confidential Information included, but is not limited to, at least the following: an identification of Plaintiffs' customers; an identification of Plaintiffs' suppliers and vendors; Plaintiffs' proprietary source code; bank account numbers; confidential internal management documents; attorney-client privileged communications in which work product, case strategy and privileged

and confidential information was discussed in *currently pending cases*; sensitive information about prior, prospective and potential business transactions, including potential company mergers or acquisitions; LIGATT Security's profit and loss reports; the social security numbers of Plaintiffs' customers and employees; personal and private information of Gregory D. Evans and Plaintiffs' employees and clients, including employment, salary, financial, credit and other personal information; and Plaintiffs' security passwords and pass codes.

36. Based on at least Plaintiffs' internal logs and files and John Doe 1's public communications, The Confidential Information was made available at The Pastebin Location at some point during the afternoon or evening of February 2, 2011 and was taken down later that day or in the early morning of February 3, 2011. The Confidential Information was stored at the Pastebin Location in password-protected files. John Doe 1 subsequently disclosed the password to the file containing The Confidential Information to a select distribution over the Internet.

37. On or about February 2, 2011 John Doe 1 issued a written statement. A copy of John Doe 1's written statement is attached hereto as Exhibit B. In his statement, John Doe 1 indicated that Mr. Evans "must be stopped by any means necessary" and expressly noted and apologized that "personal information of

many, many people [including the] [s]ocial security numbers, bank account routing numbers, credit reports, and other reports by private investigators” of “bystanders, innocent or otherwise” were contained in The Confidential Information. Upon information and belief, and at least based upon the information contained in John Doe 1’s written statement, the February 2, 2011 attack on Plaintiffs’ properties were planned to coincide with Mr. Evans’ birthday.

38. John Doe 1’s written statement was primarily directed at the Anonymous Association and encouraged recipients of the statement to refrain from publically broadcasting about the hacking so that Plaintiffs would not detect Defendants’ activities. *See* Exhibit B.

39. John Doe 1 indicated to the recipients of the statement that it was important for their activities to remain clandestine, stating that “it [is] imperative that this file be distributed as much as possible before takedown begins. *See* Exhibit B.

40. After reviewing John Doe 1’s statement and instructions, John Does 2, 4, 5, 6 and 7 downloaded or otherwise acquired The Confidential Information from the Pastebin Location. Alternatively, John Does 2, 4, 5, 6 and 7 downloaded or otherwise acquired The Confidential Information from the Pastebin Location

as a result of personal communications with John Doe 1, or obtained them directly from John Doe 1.

41. On and after February 2, 2011, Defendants continued and currently continue to access, use, possess, maintain or display The Confidential Information or allow or cause such content to be displayed at Internet web sites or accounts under their direction, control or ownership. Such access, use, possession, maintenance or display is by at least: John Doe 2's postings at the Ligattleaks Twitter Page, and the Legattleaks Homepage (exemplary copies of each are included herewith as Composite Exhibit C); the postings displayed at www.pastebin.com (exemplary copies of each are included herewith as Composite Exhibit D); John Doe 5's postings at www.attrition.com (a printout from www.attrition.com is included herewith as Exhibit E hereto); John Does 6's postings at www.twitter.com (screen images of John Doe 6's twitter posts are included herewith as Exhibit F); and John Doe 7's article located at www.thetechherald.com, disclosing Plaintiffs' confidential business information including financial information (a printout of John Doe 7's article is included herewith as Exhibit G hereto).

42. At no time relevant to this Complaint were any of the Defendants authorized by Plaintiffs to access, maintain, display or use any of The

Confidential Information in connection with the activities described herein, or for any other reason.

43. Immediately upon discovering the hacking and security breach discussed herein, Plaintiffs investigated the matter and contacted each of John Does 2, 3, 4, 5, 6 and 7, requesting that they discontinue their use, possession or display of The Confidential Information. John Does 2, 3, 4, 5, 6 and 7, however, declined to comply with Plaintiffs' request.

44. As a result of Defendants' actions, Plaintiffs have suffered and continue to suffer damage and injury to their business and reputation.

**CLAIM I – Violation of The Computer Fraud and Abuse Act
(18 U.S.C. § 1030 et. seq.) Asserted By LIGATT Securities and Spoofem
Against John Doe 1**

45. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 44 above as if fully set forth herein.

46. Without Plaintiffs' consent or authorization, and/or by exceeding any authorized access, Defendant:

- (a) intentionally or knowingly accessed a protected computer used in interstate commerce (namely Plaintiffs' Service Management Server, Web servers and the computer on which Plaintiffs' electronic mail files resided, all of which were used in interstate commerce in connection

with Plaintiffs' businesses), and obtained information from said protected computer (namely The Confidential Information) intentionally or recklessly causing damage and/or loss to each Plaintiff that exceeds \$5,000.00 in value (e.g., injury to business reputation and loss of business, as well as costs associated with repairing, diagnosing, investigating and responding to damage caused the attack, which by itself exceeds \$5,000.00) when he unlawfully accessed and stole the Confidential Information, and then posted the information on the Internet and distributed the information to others;

(b) intentionally or knowingly accessed a protected computer used in interstate commerce (namely Plaintiffs' Service Management Server, Web servers and the computer on which Plaintiffs' electronic mail files resided, all of which were used in interstate commerce in connection with Plaintiffs' businesses) with the intent to defraud obtained valuable information in excess of \$5,000 in value (e.g., The Confidential Information, use of Plaintiffs' computers and accounts);

(c) knowingly and with the intent to cause damage transmitted one or more programs, information, codes or commands to a protected computer (namely Plaintiffs' Service Management Server, Web servers,

and the computers on which Plaintiffs' electronic mail files and the files associated with Plaintiffs' Twitter account resided, all of which were used in interstate commerce in connection with Plaintiffs' businesses) and as a result of such conduct, causing or contributed to damage to and/or diminished performance of Plaintiffs' computers, computer systems, networks, accounts, facilities, information, data and have caused the withholding or denial of use of one or more of the same (e.g., loss of use of Plaintiffs' website and Twitter account).

47. As a result of Defendant's acts, Plaintiffs have suffered and continue to suffer irreparable injury, loss of reputation, and pecuniary damages to be proved at trial. Unless and until enjoined by this Court, Defendant will continue these acts, namely distributing or displaying Plaintiffs' confidential information, thereby causing Plaintiff further immediate and irreparable damage.

48. Accordingly, Plaintiffs sue Defendant under 18 U.S.C. § 1030(g) to recover for compensatory and economic damages caused by Defendant's unlawful conduct and injunctive relief as set forth below.

CLAIM II – Violation of The Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-90 et. seq.) Asserted By Mr. Evans, LIGATT Securities and Spoofem Against Defendants

49. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 48 above as if fully set forth herein.

50. John Doe 1 has committed computer theft as defined in O.C.G.A. § 16-9-93 (a) by gaining unauthorized access to Plaintiff's Service Management Server, Web servers, computer network and the computers on which Plaintiffs' electronic mail files and the files associated with Plaintiffs' Twitter account resided, for the purpose of acquiring, displaying and using The Confidential Information and perform the other acts complained of herein.

51. John Doe 1 has committed computer trespass as defined in O.C.G.A. § 16-9-93 (b) by gaining unauthorized access to Plaintiff's Service Management Server, Web servers, computer network and the computers on which Plaintiffs' electronic mail files and the files associated with Plaintiffs' Twitter account resided, for the purpose of deleting, altering, damaging or removing Plaintiffs web files and source code, electronic mail files, files stored on Plaintiffs' internal servers and causing Twitter account and websites to be temporarily inaccessible and/or unusable.

52. Defendants have committed computer invasion of privacy as defined in O.C.G.A. § 16-9-93 (c) by using computers or computer networks with the intention of examining The Confidential Information with the knowledge that Plaintiffs had not authorized such examination and that such examination was without authority.

53. Accordingly, Plaintiffs sue Defendants under O.C.G.A. § 16-9-93 (g) to recover for lost profits, the costs of this litigation and such other additional recovery of damage permitted by this statute.

**CLAIM III – Trespass to Chattels Asserted By LIGATT Securities and
Spoofer Against John Doe 1**

54. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

55. Plaintiffs' websites, email accounts, Twitter account and the computers, computer networks, and other peripheral devices and networking infrastructure that permits Plaintiff's websites, email accounts and Twitter account to function, and Plaintiffs' internal servers, constitute chattel property belonging to and/or leased by Plaintiff.

56. Defendants committed common law trespass to chattels by hacking and gaining unauthorized access to: a) Plaintiffs' web servers, maliciously

deleting files and source code necessary for the display and maintenance of the Plaintiffs' web sites, thereby rendering Plaintiffs' websites temporarily inaccessible and/or unusable ; b) Plaintiff's Twitter account, maliciously changing usernames and passwords on Plaintiff's Twitter account, and using Plaintiff's Twitter account, and thereby rendering Plaintiff's Twitter account temporarily inaccessible and/or unusable by Plaintiff; c) Plaintiffs' email files, maliciously acquiring Plaintiffs' email communications, and the documents and things attached thereto, and Plaintiffs' confidential, proprietary information and trade secrets; and d) Plaintiffs' internal network servers, maliciously acquiring Plaintiffs' confidential, proprietary information and trade secrets.

57. Plaintiffs have been damaged by Defendant's actions.

CLAIMS IV through VI – Tortious Interference Asserted By LIGATT Securities and Spoofer Against Defendants

58. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 57 above as if fully set forth herein.

59. As described herein, Defendants committed acts of theft, sabotage and cyber vandalism and other improper and illegal acts directed against Plaintiffs by: gaining unauthorized access to Plaintiffs' confidential, proprietary, and commercially sensitive information and trade secrets, Plaintiffs' online and

email accounts, and Plaintiffs' network and computers residing thereon; displaying, disseminating, acquiring or otherwise using such information and trade secrets; maliciously destroying files and source code associated with Plaintiffs' websites, and thereby rendering Plaintiffs' websites temporarily inaccessible and/or unusable; or using and/or causing Plaintiffs loss of use of Plaintiffs' Twitter account.

60. Defendants acted without privilege in their commission of the above-described acts and, at least as evidence by their own acts and admissions, acted purposefully with the intent to cause the injury to Plaintiffs complained of herein.

61. As a direct result of Defendants' conduct, Plaintiffs have already lost one or more subscription-based and other clients and have lost product sales. While Plaintiffs Internet Websites were disabled as a result of the attach set forth herein, Plaintiffs were unable to offer their products for sale or transact business online. Moreover, Plaintiffs may lose additional sales, revenue, investments, stock purchases and clients in the future due to the injury to Plaintiffs' business reputation caused by Defendants.

62. Defendants' conduct constitutes tortious interference with Plaintiffs' contractual relations and current and prospective business relations.

63. Plaintiffs have been damaged by Defendants' conduct.

CLAIM VII – Misappropriation of Trade Secrets (O.C.G.A. § 10-1-760 et seq.) Asserted By LIGATT Securities and Spoofer Against Defendants

64. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 63 above as if fully set forth herein.

65. Plaintiffs owned valuable trade secrets, as defined by O.C.G.A. § 10-1-760, in at least the confidential financial and other data, processes, business methods and practices, financial plans, product plans, and customer and supplier lists that was included as a part of The Confidential Information.

66. Defendants misappropriated Plaintiffs' trade secrets within the meaning of O.C.G.A. §10-1-761(2)(A) by acquiring The Confidential Information, or trade secret protectable portions of The Confidential Information, at the Pastebin Location, directly from John Doe 1, using other methods described herein, or otherwise, while knowing, or having reason to know, that the Confidential Information was acquired by improper means.

67. Defendants misappropriated Plaintiffs' trade secrets within the meaning of O.C.G.A. §10-1-761(2)(B) by disclosing trade secret protectable portions of The Confidential Information to third parties while, at the time of disclosure or use, knowing or having reason to know that knowledge of the trade

secret was derived by John Doe 1 or another person: 1) using improper means; 2) under circumstances giving rise to a duty to maintain its secrecy or limit its use; *or* through a person who owed a duty to Plaintiffs to maintain its secrecy or limit its use.

68. Defendant John Doe 1 misappropriated Plaintiffs' trade secrets within the meaning of O.C.G.A. §10-1-761(2)(B) by disclosing trade secret protectable portions of The Confidential Information to third parties that John Doe 1 used improper means to acquire.

69. Plaintiffs have been damaged by Defendants' conduct and are entitled to an award of damages and such other relief as permitted and/or required by O.C.G.A. §§10-1-762-64, including, but not limited to, injunctive relief, actual loss, unjust enrichment and attorney's fees. Because Defendants' conduct recited herein was willful and malicious, Plaintiffs are further entitled to an award of enhanced damages as provided by O.C.G.A. §§10-1-763(b).

COUNT VIII - Conversion Against Defendants

70. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 69 above as if fully set forth herein.

71. Plaintiffs owned, possessed, and/or had the right of immediate possession of various items of intangible and tangible personal property,

including, but not limited to Plaintiffs' trade secrets, confidential and proprietary business information, and one or more company computers, Plaintiffs' e-commerce web sites and online account at Twitter.com.

72. Based at least on Defendants' own admissions and Internet postings, John Doe 1 maintained and/or maintains actual possession of all of the foregoing property of Plaintiffs, and each Defendant maintained and/or maintains possession of Plaintiffs' trade secrets, and confidential and proprietary business information.

73. Plaintiffs have made a demand of each of the Defendants regarding the return of the foregoing property, and Defendants have refused such demands, and Plaintiffs have suffered and continue to suffer damages as a result.

74. At least by virtue of Defendants' own admissions and Internet postings, and the nature of the alleged activities (e.g., hacking), Defendants knowingly took possession of property of which Plaintiffs were unlawfully dispossessed.

**COUNT IX - Attorney Fees (O.C.G.A. § 13-6-11) Asserted By Mr. Evans,
LIGATT Securities and Spoofer Against Defendants**

75. Plaintiffs re-allege and incorporates by reference the allegations contained in Paragraphs 1 through 74 above as if fully set forth herein.

affirmative representations that their acts were intentional, Defendants' use of aliases and the lengths to which Defendants have gone and continue to go to mask their identity, and the nature of the alleged activities (e.g., hacking), Defendants have acted with willful misconduct, malice, fraud, wantonness, oppression, and/or that entire want of care which raises a presumption of conscious indifference to the consequences of their actions.

81. Based at least on the items of evidence in the immediately preceding Paragraph: Defendants knew that their intentional wrongful acts would cause substantial harm to Plaintiffs; Defendants intended the consequences of their actions; and Defendants' wrongful acts were done to cause financial and business injury and disruption to Plaintiffs and bring notoriety to themselves at Plaintiffs' expense.

82. Given the egregious and intentional nature of Defendants' conduct, Plaintiff is entitled to an award of punitive damages pursuant to O.C.G.A. § 51-12-5.1 to punish and penalize these Defendants, to deter these Defendants from similar future misconduct, and to deter other hackers, persons and entities similarly situated to Defendants from engaging in future misconduct like that of Defendants.

**COUNT XI - Civil Conspiracy Asserted By Mr. Evans, LIGATT
Securities and Spoofem Against Defendants**

83. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 82 above as if fully set forth herein.

84. Defendants have engaged in a concert of action for the purposes of committing the tortuous, illegal and improper conduct described herein.

Defendants understood and agreed to pursue a course of action which had the common purpose and objective of committing such conduct, including but not limited to the acquisition, display and/or use of the Confidential Information for their own commercial advantage and notoriety and with a specific intent to harm Plaintiff. Defendants affiliated with one another, participated and engaged in, supported, authorized, and/or ratified such acts of misappropriation, and conversion, and for the purpose of continuing and perpetrating the wrongful conduct described above.

85. Such conduct constitutes actionable civil conspiracy in that Defendants carried out lawful and unlawful transactions by unlawful means. As conspirators, Defendants are responsible for all conduct undertaken in furtherance of the conspiracy regardless of whether each particular Defendant performed, authorized, had knowledge of or directed such conduct. Such

conduct makes all Defendants jointly and severally liable to Plaintiffs. In addition, because Defendants' actionable civil conspiracy was formed, implemented, and executed knowingly, intentionally, willfully and/or maliciously, Plaintiffs seek to recover an additional amount in the form of punitive and exemplary damages against Defendants.

PRAYER FOR RELIEF

WHEREFORE, by virtue of the unlawful conduct of Defendants as alleged in Counts I through XI of this Verified Complaint, Plaintiffs respectfully pray that:

A. Defendants be required to pay Plaintiffs actual damages, compensatory damages, and any other statutory damages recited, required or permitted by any applicable provision of the Georgia Code and/or the United States Code;

B. The Court enter temporary, preliminary, and thereafter permanent injunctions enjoining Defendants, their agents, employees, and/or representatives, and all those in active concern or participation with them, from using, possessing, transferring, transmitting, conveying, selling, or displaying any of The Confidential Information and as requested in Plaintiffs' Motion for Temporary Restraining Order submitted contemporaneously herewith;

C. Defendants be required to provide to Plaintiffs and this Court an accounting, verified under penalty of perjury, of their use(s) of Plaintiff's private, confidential, and proprietary information and trade secrets;

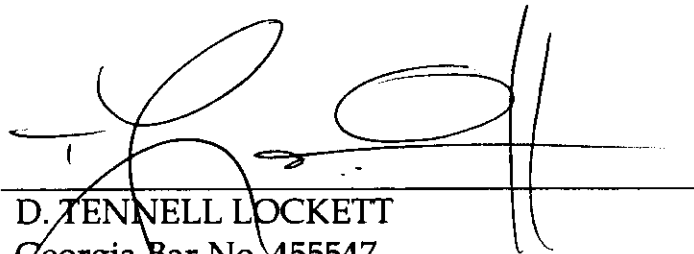
D. prejudgment and post-judgment interest as provided for by law;

E. Defendants be required to pay Plaintiffs the costs of this action and the reasonable attorneys' fees Plaintiffs have incurred in connection with this action;

F. Defendants be required to pay Plaintiffs enhanced damages and punitive damages in light of the willful and predatory nature of Defendants' actions; and

G. Plaintiffs be granted such other, different and additional relief as the Court deems just and proper.

Respectfully submitted this 15th day of February, 2011.



A handwritten signature in black ink, consisting of a large, stylized 'D' followed by a horizontal line and a vertical stroke.

D. TENNELL LOCKETT
Georgia Bar No. 455547

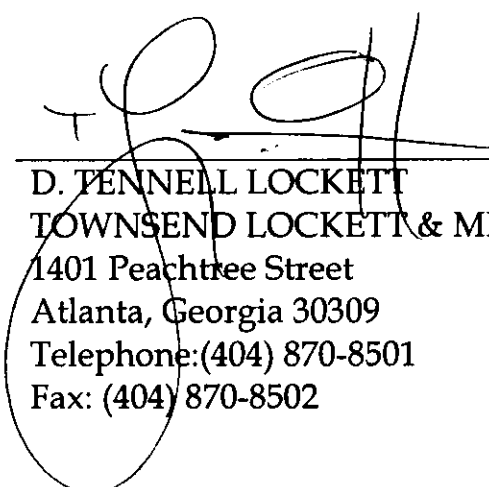
TOWNSEND LOCKETT & MILFORT, LLC
1401 Peachtree Street
Atlanta, Georgia 30309
Telephone: (404) 870-8501
Fax: (404) 870-8502
tennell.lockett@townsendlockett.com

Attorneys for Plaintiffs Gregory D. Evans,
LIGATT Security International, Inc. and
Spoofem.com USA Inc.

JURY DEMAND

The Plaintiffs hereby request trial by jury on all issues triable to a jury.

Respectfully submitted this 5th day of February, 2011.



D. TENNELL LOCKETT
TOWNSEND LOCKETT & MILFORT, LLC
1401 Peachtree Street
Atlanta, Georgia 30309
Telephone: (404) 870-8501
Fax: (404) 870-8502

Attorneys for Plaintiffs.

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**GREGORY D. EVANS, LIGATT
SECURITY INTERNATIONAL,
INC., and SPOOFEM.COM USA
INC.,**

Plaintiffs,

vs.

JOHN DOES 1-8,

Defendants.

§
§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. _____


FILED UNDER SEAL

VERIFICATION


Personally appeared before me, the undersigned officer duly authorized by law to administer oaths, Gregory D. Evans, President and Chief Executive Officer of LIGATT Security International, Inc. and Spoofer.com USA Inc. ("LIGATT"), who having been duly sworn, deposes and states the following:

I am Gregory D. Evans. I have read the foregoing Verified Complaint, reviewed the relevant and pertinent business records of LIGATT kept in the ordinary course of its business, and have spoken with appropriate employees of LIGATT. Based upon my personal knowledge and investigation, I can state that the facts contained in the Verified Complaint are true and correct.

This 14th day of February 2011.


GREGORY D. EVANS
CHIEF EXECUTIVE OFFICER
LIGATT SECURITY INTERNATIONAL, INC.
SPOOFEM.COM USA INC.

Sworn to and subscribed before me
this 14th day of February 2011.


Notary Public

My Commission Expires:

02/04/2012

