

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

FEB 15 2011

JAMES M. HATTEN, Clerk  
By: [Signature] Deputy Clerk

**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.**

**111 · CV - 0458**

**FILED UNDER SEAL**

**DECLARATION OF GREGORY D. EVANS**

I, GREGORY D. EVANS, pursuant to 28 U.S.C. §1746, hereby affirm that I am over 18 years of age and I am competent to make the following Declaration:

1.

This Declaration is based on my personal knowledge. I hereby swear, under penalty of perjury, that the allegations contained herein and in the Verified Complaint are true and accurate to the best of my knowledge, information and belief.

2.

I am a Georgia resident and Chief Executive Officer of LIGATT Security

International, Inc. ("LIGATT") and Spoofem.com USA, Inc. ("Spoofem"). I founded LIGATT in 2003 and founded Spoofem in 2006.

3.

LIGATT is a California corporation that is duly licensed to conduct business in the State of Georgia. LIGATT's principal place of business is located at 6991 Peachtree Industrial Boulevard, Norcross, Gwinnett County, Georgia.

4.

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.

LIGATT and Spoofem are small closely-held companies that have grown into nationally-renowned, publically-traded companies.

6.

LIGATT has 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. LIGATT offers a number of cutting-edge security products directly to its customers at its website, located at [www.ligattsecurity.com](http://www.ligattsecurity.com), and through various third-party vendors. LIGATT'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 has become well-known in the information security industry for its products and services, including, by way of example, its Locate PC product.

7.

Spoofem, a sister-company to LIGATT, 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.

8.

At their websites, maintained at [www.ligattsecurity.com](http://www.ligattsecurity.com) and [www.spoofem.com](http://www.spoofem.com) respectively, LIGATT and Spoofem, among other things: (a) offer goods and services for sale; (b) transact online product purchases; (c) provide marketing and other informational materials about their products and companies; and (d) provide a link that directs users to a location where end users can purchase public shares of each respective company. LIGATT and Spoofem maintain a web

server at their business location that hosts their business websites. LIGATT and Spoofer also maintain at their business location a centralized server that houses company confidential and proprietary business information and private personal information (the "Service Management Server").

9.

As LIGATT and Spoofer's business and notoriety expanded over the years, so has my professional reputation as a digital and network security expert.

10.

Through my many years of hard work in building and developing LIGATT and Spoofer, and other related undertakings, I have 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.

11.

My successes as a newcomer and quick-riser in the information security market to have caused some market actors some degree of resentment and angst. (See, e.g., Exhibit A to the Verified Complaint filed in this action.)

12.

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 me and my businesses (the “Anonymous Association”).

13.

The Defendants in this action are “unknown” individuals who reside in various states within the United States. Defendants have concealed their identity and whereabouts by creating and posting content on the Internet using aliases.

14.

Without authorization, Defendants, individually or collectively, have 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. Defendants have also disclosed that information to third-parties on the Internet as more fully described in the Verified Complaint.

15.

Defendants, either individually or collectively, own, operate, administer, use or maintain 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 maintain and use an account at the real-time information network provided at [www.twitter.com](http://www.twitter.com) under the alias “ligattleaks” (the “Ligattleaks Twitter Page”).

16.

One or more of the Defendants owns, uses or controls the email account associated with the address [ligattleaks@hushmail.com](mailto:ligattleaks@hushmail.com).

17.

Defendants, either individually or collectively, also own, operate, administer, use or maintain the website located at [www.pastebin.com](http://www.pastebin.com).

18.

One or more of the Defendants owns, uses or controls the email account associated with the address [pastebin@gmail.com](mailto:pastebin@gmail.com).

19.

One or more of the Defendants owns, operates, administers, uses or maintains one or more user or posting accounts at the website located at [www.pastebin.com](http://www.pastebin.com).

20.

One or more of the Defendants owns, operates, administers, uses or maintains a website located [www.attrition.org](http://www.attrition.org) and uses an account at the real-time information network provided at [www.twitter.com](http://www.twitter.com) under the alias "attritionorg" (the "Attrition Twitter Page").

21.

One or more of the Defendants uses an account at the real-time information network provided at [www.twitter.com](http://www.twitter.com) under the alias "lucky225" (the "Lucky225 Twitter Page").

22.

One or more of the Defendants owns, operates, administers, uses or maintains the website located at [www.thetechherald.com](http://www.thetechherald.com). Based on information provided at [www.thetechherald.com](http://www.thetechherald.com), I believe that at least one of the Defendants uses or maintains a physical address located at 320 N Parker Avenue, Indianapolis, IN 46201.

23.

One or more of the Defendants accessed, downloaded, reviewed or otherwise acquired The Confidential Information (to be later defined) at The Pastebin Location (to be later defined).

24.

One or more of the 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 the Verified Complaint toward Georgia.

25.

In particular, Defendants gained unauthorized access (hacked) into LIGATT and Spoofer's computers, which are located in Georgia, and used said access to view and copy information and stored communications, and to assume control of various of LIGATT and Spoofer's online accounts and shutdown our e-commerce website. Such conduct has caused LIGATT, Spoofer, and their customers significant harm. Defendants have undertaken these 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.

26.

As part of its efforts to maintain an online presence and increase brand interest and loyalty, LIGATT uses and maintains an account with the online service provider operating at [www.twitter.com](http://www.twitter.com). At all times relevant to the



Verified Complaint filed in this action, LIGATT's Twitter account was password protected and LIGATT's practice permitted restricted access to the company's Twitter account.

27.

At all times relevant to the Complaint filed in this action, both LIGATT and Spoofem maintained 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 the personal information of Plaintiffs' customers, Plaintiffs' vendors and Plaintiffs' employees.

28.

Both LIGATT and Spoofem have taken considerable 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, but not limited to 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. Both LIGATT and Spoofem also require all of its employees to execute confidentiality agreements.

29.

A “hacker” is someone who subverts computer security without authorization or who uses technology (usually a computer or the Internet) for various reasons including, 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.”

30.

“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.

31.

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 then 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.

32.

Defendants have engaged in “hacking” of Plaintiffs’ computer security systems and/or the “cracking” of my user passwords in order to gain unauthorized access to and trespass upon my Companies’ website, systems and/or network.

33.

In particular, on or about February 2, 2011, one or more of the Defendants accessed Plaintiffs’ private business network by means of hacking or cracking (hereinafter, collectively referred to as “hacked” or “hacking”).

34.

On or about February 2, 2011, Defendants also 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, one or more of the Defendants downloaded, copied or otherwise acquired confidential, proprietary, and commercially sensitive from the Service Management Server, including at least passwords and pass codes to various virtual and physical company locations that housed additional confidential information. Defendants 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.

35.

As a direct result of Defendants' unlawful actions, LIGATT and Spoofer's websites were unavailable from the time of the hacking on February 2, 2011 until on or about February 8, 2011.

36.

On or about February 2, 2011, one or more of the Defendants accessed LIGATT and Spoofer's email accounts by means of hacking, and downloaded, copied or otherwise acquired in excess of 80,000 company emails, attachments included, stored in my company email accounts. The emails contained in my accounts dated back at least 5 years and contained countless attachments and communications discussing and disclosing proprietary, confidential, commercially sensitive and private information.

37.

On or about February 2, 2011, one of more of the Defendants accessed LIGATT's Twitter account and took control over the account, changing the account's user name and password. After assuming control of the account, one or more of the Defendants issued several statements from LIGATT's Twitter account,

impersonating Mr. Evans and providing a link to the url <http://pastebin.com/raw.php?i=3k8jrMJn> (the "Pastebin Location").

38.

After downloading, copying or otherwise acquiring the aforementioned files, data and information belonging to Plaintiffs ("The Confidential Information"), one or more of the Defendants posted or otherwise made available The Confidential Information at the Pastebin Location. In so doing, Defendants 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 to the Verified Complaint filed in this action).

39.

The Confidential Information included, but is not limited to, at least the following: (a) an identification of Plaintiffs' customers (i.e., customer list); (c) an identification of Plaintiffs' suppliers and vendors; (c) Plaintiffs' proprietary source code; (d) bank account numbers; (e) confidential internal management documents; (f) attorney-client privileged communications in which work product, case strategy and privileged and confidential information was discussed in currently pending cases; (g) sensitive information about prior, prospective and potential business

transactions, including potential company mergers or acquisitions; (f) LIGATT's profit and loss reports; (g) the social security numbers of Plaintiffs' customers and employees; (h) my personal and private information, including information relating my private relationships, credit reports, private information regarding my child and their medical history and examinations, and other such private and personal information; and (i) personal information of Plaintiffs' employees and clients, including employment, salary, financial, credit and other personal information; and Plaintiffs' security passwords and pass codes. Each of the foregoing are kept secret, private, secure and confidential. At least Plaintiffs customer list, source code, vendor and supplier list, product and business plans are valuable assets of the LIGATT Security and Spoofer and maintain all or some of their value by virtue of their confidential nature. For example, the customer list has been built from the inception of LIGATT Security and consists of repeat customers, choice customers and the like. Such list would be of value to a competitor in my field.

40.

Based on at least Plaintiffs' internal logs and files and Defendants' 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. See Attachment 1 hereto (noting that, at least 8 hours after the attack, Pastebin files were removed). The Confidential Information was stored at the Pastebin Location in password-protected files. Defendants subsequently disclosed the password to the file containing The Confidential Information to a select distribution over the Internet.

41.

On or about February 2, 2011, one or more of the Defendants issued a written statement. A copy of this written statement is attached to the Verified Complaint as Exhibit B. The statement indicated that I “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. The February 2, 2011 attack on LIGATT and Spoofer’s properties were carefully planned to coincide with my birthday.

42.

Defendants’ 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 to the Verified Complaint).

43.

Defendants 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 to the Verified Complaint).

44.

Defendants downloaded or otherwise acquired The Confidential Information from the Pastebin Location. *See* Paragraph 46 hereto.

45.

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.

46.

Such access, use, possession, maintenance or display is shown by:

(a) at least one of the Defendants' postings at the Ligattleaks Twitter Page, and the Legattleaks Homepage (exemplary copies of each are attached to the



Verified Complaint as Exhibit C) and the pasting entitled "Keep Leaking Legal Advice From D.C. Counsel" (Attachment 2 hereto at 3);

(b) the postings displayed at [www.pastebin.com](http://www.pastebin.com) (exemplary copies of each are attached to the Verified Complaint as Composite Exhibit D);

(c) Defendants' postings at [www.attrition.com](http://www.attrition.com) (a printout from [www.attrition.com](http://www.attrition.com) is attached to the Verified Complaint as Exhibit E);

(d) Defendants' postings at [www.twitter.com](http://www.twitter.com) (screen images of said twitter posts are attached to the Verified Complaint as Exhibit F); and

(e) Defendants' article located at [www.thetechherald.com](http://www.thetechherald.com), disclosing Plaintiffs' confidential business information including financial information (a printout of said article is attached to the Verified Complaint as Exhibit G).

47.

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.

48.

Immediately upon discovering the hacking and security breach discussed herein, Plaintiffs investigated the matter and contacted each of the Defendants,

requesting that they discontinue their use, possession or display of The Confidential Information. *See, e.g.,* Attachment 3 hereto (exemplary communication). However, Defendants declined to comply with Plaintiffs' request. *See, e.g.,* Attachment 4 hereto (exemplary response).

49.

As a result of Defendants' malicious actions, Plaintiffs have suffered and continue to suffer damage and injury to their business and reputation. For example, beginning on February 3, 2011, we have lost multiple customers, both existing and potential, that expressly stated that the reason that they chose to discontinue, decline or request a refund for our products or services was due to our recent breach and security issue. Additionally, one of my competitors, Kevin Mitnick, transmitted a communication on Twitter.com inquiring as to whether there was any discovery of my companies' client list. *See* Attachment 5 hereto at Tweet 147.


50.

I have run "WHO IS" searches for the domains<ligattleaks.com>, <ligattleaks.org>, <ligattleaks.net>, <pastebin.org>, <thetechherald.com> and <attrition.org> and have attached true and correct copies of the same hereto as Attachment 6.

51.

I have read and understand this Declaration, consisting of **FIFTY-ONE (51)** numbered paragraphs. Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 14, 2011.

  
GREGORY D. EVANS