

Specifically, a yet unknown Defendant hacked into the corporate offices of two of the most well-known and well-regarded companies in the information security industry, LIGATT Security International, Inc. ("LIGATT Security") and Spoofem.com USA, Inc. ("Spoofem"). After breaching the companies' substantial security measures, the assailant took down the companies' websites, downloaded easily in excess of 80,000 personal and corporate files, documents and records, pirated LIGATT Security's Twitter account and absconded with countless pieces of personal, private, proprietary, confidentially and highly-sensitive corporate information and trade secrets ("The Confidential Information").

When Defendant completed the theft, he shared The Confidential Information with his friends and associates, openly and brashly bragging about the source of the information and how it was obtained. Despite knowing that this information was private, proprietary, confidential and admittedly stolen, Defendants downloaded, reviewed, used, and, in some instances, shared the stolen content with others. Indeed, at least one Defendant openly encouraged others to download, use and review the stolen goods in the hopes that the magic of the Internet could somehow cause their later illegal acts to pardon their prior illegal acts. Fortunately, the law does not permit such a result.

Although it is wrapped in a new-millennium air of high-tech sophistication, Defendants' conduct simply amounts to plain old theft; theft and knowingly receiving and using stolen property. And thankfully for Plaintiffs and other holders of private, confidential, proprietary and trade secret information, the law still protects against such violations, even when they occur over the Internet.

Despite Plaintiffs' efforts to resolve this issue amicably, Defendants have made it clear that they will continue their conduct unabated, and to the detriment of Plaintiffs. Because Defendants' conduct is directed to the possession, display, distribution or use of Plaintiffs' confidential and private information and trade secrets, every day that Defendants are permitted to continue their unlawful and unauthorized use of The Confidential Information, Plaintiffs will continue to suffer substantial irreparable harm to its reputation, goodwill and business. Plaintiffs therefore request that this Court temporarily and thereafter preliminarily enjoin Defendants from further use of The Confidential Information in any manner, as more fully set forth in Plaintiffs' Motion filed herewith.

FACTUAL BACKGROUND

In addition to the facts contained in Plaintiffs' Verified Complaint, filed contemporaneously herewith, Plaintiffs recites the following information and facts.

I. PLAINTIFFS AND THEIR BUSINESSES

Since their inceptions, LIGATT Security and Spoofem have 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. Declaration of Gregory D. Evans ("Evans Decl.") at ¶6. 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. *Id.* 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. *Id.* at ¶7.

Plaintiffs' websites, located at www.ligattsecurity.com and www.spoofem.com, were and are e-commerce sites. *Id.* at ¶8. 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 personal information (the "Service Management Server"). *Id.*

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. *Id.* at ¶26. 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. *Id.*

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. *Id.* 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. *Id.*

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. *Id.* at ¶28. Plaintiffs also use a system and process to protect the confidential, private and proprietary information in its ownership and control that incorporates 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. Evans Decl. at ¶28.

II. DEFENDANTS AND THEIR MISCONDUCT

On or about February 2, 2011, John Doe 1 (as identified in Plaintiffs' Complaint) accessed Plaintiffs' private business network by means of hacking or cracking (hereinafter, collectively referred to as "hacked" or "hacking"). *Id.* at ¶34.

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. *Id.* After hacking into Plaintiffs' network, John Doe 1 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. *Id.* 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. *Id.* 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. *Id.* at ¶35.

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. *Id.* at ¶36. 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. *Id.*

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. *Id.* at ¶37. 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"). *Id.*

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. *Id.* at ¶38. 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. *Id.* at ¶38.

The Confidential Information included, but is not limited to, at least the following: an identification of Plaintiffs' customers, such customer list including over 100,000 of Plaintiffs' customers; an identification of Plaintiffs' suppliers and vendors; Plaintiffs' proprietary source code (including the source code for its Popular Locate PC software); 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. Evans Decl. at ¶39.

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. *Id.* at ¶40. The

Confidential Information was stored at the Pastebin Location in password-protected files. *Id.* John Doe 1 subsequently disclosed the password to the file containing The Confidential Information to a select distribution over the Internet. *Id.*

On or about February 2, 2011 John Doe 1 issued a written statement. *Id.* at ¶41. 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. *Id.* 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. *Id.*

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. *Id.* at ¶42.

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. *Id.* at ¶42-43.

After reviewing John Doe 1's statement and instructions, John Does 2, 4, 5, 6, 7 and 8 downloaded or otherwise acquired The Confidential Information from the Pastebin Location. *Id.* at ¶44. Alternatively, John Does 2, 4, 5, 6, 7 and 8 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. *Id.*

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 websites or accounts under their direction, control or ownership. *Id.* at ¶45-46. 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; the postings displayed at www.pastebin.com; John Doe 5's postings at www.attrition.com; John Does 6's postings at www.twitter.com; and John Doe 7's article located at www.thetechherald.com, disclosing Plaintiffs' confidential business information including financial information. *Id.*

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.

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.

ARGUMENT AND CITATION OF AUTHORITIES

For temporary or preliminary injunctive relief to be warranted, Plaintiffs must demonstrate:

- (1) a substantial likelihood of success on the merits;
- (2) a substantial threat that Plaintiffs will suffer irreparable injury if the requested relief is not granted;
- (3) the injury to Plaintiffs is greater than any damage an injunction may cause Defendants; and
- (4) the injunction will serve the public interest.

See, e.g., Frio Ice, S.A. v. Sunfruit, Inc., 918 F.2d 154, 159 (11th Cir. 1990). As show below, Plaintiffs' motion satisfies each of these four prerequiCites.

I. PLAINTIFFS ARE SUBSTANTIALLY LIKELY TO PREVAIL ON THE MERITS OF THEIR CLAIMS.

As set forth below, Plaintiffs are substantially likely to prevail on each of their claims. To be entitled to relief, however, Plaintiffs need only show a substantially likelihood of success on one of the claims that have brought against Defendants.

A. Plaintiffs Are Likely to Prevail On the Merits of Their Case Under the Georgia Trade Secrets Act (O.C.G.A. § 10-1-760 et seq.).

To recover for misappropriation of trade secrets under the Georgia Trade Secrets Act, Plaintiffs must prove that (1) it had a trade secret as defined by O.C.G.A. § 10-1-761(4); and (2) Defendants misappropriated that trade secret. *Penalty Kick Management v. Coca Cola Co.*, 318 F.3d 1284, 1290-1291 (11th Cir. 2003). Plaintiffs' claims readily satisfy both requirements.

1. Plaintiffs Have Protectable Trade Secret Rights.

There can be no dispute that The Confidential Information includes one or more categories of information covered by the Georgia Trade Secret Act. The Confidential Information at least includes: Plaintiffs' customer lists; Plaintiffs' proprietary and confidential source code in one or more of its products, including its popular Locate PC product; the company's financial records, including profit and loss reports. Evans Decl. at ¶39. On its face, O.C.G.A. § 10-1-761(4) defines "[t]rade secret[s]" to include "a program," "financial data," "financial plans," "product plans" and "a list of actual or potential customers or suppliers." See O.C.G.A. § 10-1-761(4). Indeed, The Confidential Information included, among other things, a database of over 100,000 of Plaintiffs' customers. Evans Decl. at ¶38.

The Georgia Trade Secrets act further provides that such material may qualify as trade secrets if it "is not commonly known by or available to the public," and: "(A)

Derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (B) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." O.C.G.A. § 10-1-761(4).

Plaintiffs' customer lists, source code, product plans, financial information, etc. are valuable assets to Plaintiffs and undoubtedly derive economic value from not being generally known or readily known ascertainable by proper means to those in the industry. *Id.* at ¶39. Plaintiffs' customer list, for example, comprise over 100,000 individuals and was acquired over an 8-year period. *Avnet, Inc. v. Wyle Labs.*, 263 Ga. 615, 616-617(1) (1993) (holding that lists containing the identities of, and specific information concerning, an employer's actual customers are considered a trade secret where the employer "ha[s] made a reasonable effort to maintain the secrecy of the customer lists"). Indeed, its value is at least evidenced by Plaintiffs' competitor's interest in it. *Evans Decl.* at ¶39. Likewise, Plaintiffs have confidential and proprietary source code running on one or more of its products that was developed or acquired by Plaintiffs through considerable expense and effort.

There can also be very little dispute that Plaintiffs took reasonable efforts under the circumstances to maintain the secrecy of its information. For example, Plaintiffs have each and every one of their employees sign confidentially agreements, agreeing to

keep such information confidential, keep password protection on any virtual locations storing confidential materials and keep a separate password and encryption system protecting access to the network on which such locations reside. Evans Decl. at ¶28. Plaintiffs further employ physical barriers to information that is physically stored in the office, maintaining such information in locked locations and further implementing a series of door-codes to prevent access to certain areas. Evans Decl. at ¶28. Plaintiffs also limit access to certain files that have a higher degree of sensitivity, such as customer lists and files use password protections, to restricted personnel and such access if provided on a need-to-know basis. *Id.* Such efforts satisfy the “reasonable efforts” requirement of the statute. *Specialty Chemicals & Serv., Inc. v. Chandler*, No. 1:87CV-2338, WL 618583 at *5 (N.D.Ga.) (N.D. Ga. Sept. 29, 1988) (reasonable efforts meet where trade secrets kept secure “under lock and key,” and access to trade secrets limited to authorized personnel); *Paramount Tax & Accounting, LLC v. H & R Block Eastern Enter., Inc.* 299 Ga.App. 596, 603 (Ga. App. 2009) (reasonable efforts found where there was access to customer database was limited to certain employees and the information was password protected).

The only reasonable question concerning Plaintiffs’ trade secret is whether the information somehow lost its trade secret status (e.g., became public information) by virtue of Defendants’ distribution. The answer to that question is “no.” As an initial

matter, Defendants may not, in an effort to avoid penalty, publish Plaintiffs' trade secret and simultaneously claim that acts absolve them of liability, such an end-run is not permitted by law. *Paramount Tax & Accounting, LLC v. H & R Block Eastern Enter., Inc.* 299 Ga.App. 596, 604 (Ga. App. 2009) (accused could not benefit from its misappropriation of a competitor's trade secrets). Because Defendants were part of any effort to display Plaintiffs' trade secrets, such a defense will not assist them. *Id.*

More to the point, however, is that John Doe 1's February 2, 2011 post of the Confidential Business Information to the Pastebin Location did not destroy the trade secrets held by Plaintiffs in The Confidential Business Information. John Doe 1 informed a limited number of individuals about the posting, password protected the file containing the Confidential Business Information, circulated the password to certain individuals via separate communication and well after the initial upload, and made it abundantly clear to those looking to access the information that the information was pilfered and contained confidential, private and proprietary information. Evans Decl. at ¶ 40-42 (requesting that those participating refrain from publically posting about the theft to prevent Plaintiffs from discovery the theft). Moreover, the password protected file was up on the Internet for a matter of hours, being uploaded the afternoon of February 2, 2011 and taken down the following morning. *Id.* at 40.

Because the disclosure was limited in time, scope and availability as set forth above, any trade secrets that Plaintiffs had in The Confidential Information survived John Doe 1's posting. Importantly, trade secret law recognizes that information does not have to retain total secrecy in order to maintain protection. *See Tronitec, Inc. v. Shealy*, 249 Ga. App. 442, 451 (2001) (holding that protection was not waived where the information was unsealed in open court records for a short time, because "while court records may be available to the public, there is no general dissemination of such information"), *overruled on other grounds, Williams Gen. Corp. v. Stone*, 279 Ga. 428 (2005). As such, any individual that downloaded, used or displayed the information uploaded by John Doe 1 did so in violation of trade secret law. Moreover, while it is Plaintiffs' position that none of their trade secrets have been rendered forfeit by Defendants' or anyone else's conduct, it is worth noting that the greater majority of the over 80,000 emails and information have not yet been displayed.

2. Defendants have Misappropriated Plaintiffs' Trade Secrets.

Under the Georgia Trade Secret Act, misappropriate means:

- (A) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
- (B) Disclosure or use of a trade secret of another without express or implied consent by a person who:
 - (i) Used improper means to acquire knowledge of a trade secret;
 - (ii) At the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was:

- (I) Derived from or through a person who had utilized improper means to acquire it;
- (II) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
- (III) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
- (iii) Before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

O.C.G.A. § 10-1-761(2).

Because each Defendant has downloaded (i.e., acquired) The Confidential Information and, by the very nature of the act and the type of information stored at the Pastebin Location, knew or, at the very least, *had reason to know*, that the trade secret was acquired by improper means in violation of O.C.G.A. § 10-1-761(2)(A). Evans Decl. at ¶44. Any possibility of ignorance as to the circumstances under which Plaintiffs' information was being provided, and the contents thereof, was put to rest by John Doe 1's brazen written statement, informing individuals of the posted file and detailing his activity. *Id.* at 41. Because Defendants reviewed The Confidential Information and posted samples of The Confidential Information under the same circumstances, Defendants' conduct further violates at least O.C.G.A. § 10-1-761(2)(B)(i),(ii)(I).

B. Plaintiffs Are Likely to Prevail On the Merits of Their Case Under the Violation of The Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-90 et. seq.).

O.C.G.A. §16-9-93(g) creates a private cause of action for any person whose property or person is injured by reason of:

(a) *Computer theft*. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

- (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;
- (2) Obtaining property by any deceitful means or artful practice; or
- (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property

shall be guilty of the crime of computer theft.

(b) *Computer Trespass*. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

- (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
 - (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or
 - (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists
- shall be guilty of the crime of computer trespass.

(c) *Computer Invasion of Privacy*. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

See O.C.G.A. §16-9-93(a),(b),(c) and (g).

While sub-sections (a) and (b) of O.C.G.A. §16-9-93 are directed to the *use* of a computer without authority, sub-section (c) merely requires that a person uses a computer with the intention of *examining* employment, medical, salary, credit or any other financial information or personal data, where the person knew that their examination was without authority.

Here, there can be very little dispute that each individual intended to examine at least the personal data of at least Mr. Evans and knew that they were not authorized by Mr. Evans, or otherwise, to access, examine and review The Confidential Information. The Confidential Information was replete with Mr. Evans' personal information, including private and personal communications regarding his personal relationships, his child's medical examinations, personal credit report and other private issues. Evans Decl. at ¶39. It can hardly be argued that such information does not constitute data, as the Act expressly defines "Data" to "include any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network." O.C.G.A. §16-9-92(5).

That Defendants knew that The Confidential Information contained Mr. Evans' personal information and that they were unauthorized to examine such files is evidence at least by John Doe 1's request that Defendants conceal their activities, that

none of the Defendants contacted Mr. Evans or anyone at Plaintiffs' business to inform him of this posting, and by their continued access and review of such files after their initial examination. Accordingly, Plaintiffs are likely to prevail on their claims.

C. Plaintiffs Are Likely to Prevail on their Conversion Claim.

To prevail on their conversion claim, Plaintiffs must show (1) title to the property or the right of possession, (2) actual possession in the other party, (3) demand for return of the property, and (4) refusal by the other party to return the property. *See Hooks v. Cobb Center Pawn & Jewelry*, 241 Ga. App. 305, 308(5), 527 S.E.2d 566 (1999). Plaintiffs' case here is straightforward. There can be no legitimate dispute that Plaintiffs own a valuable property right in The Confidential Information and Defendants, through their various postings and admissions make clear that they are in possession of The Confidential Information. Evans Decl. at ¶44, 46. Plaintiffs have requested that at least John Doe 2, John Doe 3, John Doe 5, John Doe 6 and John Doe 7 to return, discontinue the use of, destroy, or delete The Confidential Information. *Id.* at ¶48. As of the date of this filing, Defendants have continued to decline such demand. *Id.*

D. Plaintiffs Are Likely to Prevail on their Tortious Interference Claim.

As with its conversion claim, Plaintiffs' claims here are equally straightforward. Tortious interference claims, whether asserting interference with contractual relations, business relations, or potential business relations, share certain common

essential elements: (1) improper action or wrongful conduct by the defendant without privilege; (2) the defendant acted purposely and with malice with the intent to injure; (3) the defendant induced a breach of contractual obligations or caused a party or third parties to discontinue or fail to enter into an anticipated business relationship with the plaintiff; and (4) the defendant's tortious conduct proximately caused damage to the plaintiff. *Fortson v. Brown*, 302 Ga.App. 89, 92 (Ga. App. 2010).

As demonstrated above, Defendants improperly accessed, downloaded, used and acquired Plaintiffs' personal, confidential, private, proprietary information and trade secrets. Defendants had no legitimate basis or right to do so. Likewise, for reasons previously discussed, Defendants' conduct was undoubtedly with malice and with intent to injure and damage Plaintiffs. Plaintiffs have already suffered substantial and significant monetary and other damage and injury as a result of Defendants' conduct, including actual lost sales from one or more prospective and existing customers, who expressly attributed the incident described herein as the reason for their decision to either decline, request a refund for, or discontinue their services with Plaintiffs. Evans Decl. at ¶49.

II. PLAINTIFFS WILL SUFFER SUBSTANTIAL IRREPARABLE HARM IF ITS MOTION IS DENIED.

In trade secret cases such as the instant matter, irreparable harm is necessarily present. Defendants here have shown an open disregard for Plaintiffs' confidential and

trade secret information and have stated in no uncertain terms that they will continue to use Plaintiffs' trade secrets. *See Id.* at ¶46 (stating that Defendants were free to continue using Plaintiffs' information and encouraging others to "KEEP LEAKING!"). As noted by this Court, "the mere threat of disclosure, destruction or dilution of a plaintiff's trade secrets creates irreparable injury justifying injunctive relief." *Specialty Chemicals & Serv., Inc. v. Chandler*, No. 1:87CV-2338, WL 618583 at *5 (N.D.Ga.) (N.D. Ga. Sept. 29, 1988) (internal citations omitted). There is no genuine debate here that Defendants, by their own admissions, possess Plaintiffs' trade secrets and intend on displaying and using them, thereby establishing irreparable injury. *Id.*

Furthermore, the Defendants have openly and unashamedly used Plaintiffs' trade secrets in the past. "Prior use of misappropriated trade secrets is sufficient evidence of likely irreparable harm to support injunctive relief." *Id.*

In this case, the irreparable harm to Plaintiffs goodwill and business reputation is particularly egregious. LIGATT Security and Spoofem are in the information security industry. Each day that Defendants are permitted to continue using and posting Plaintiffs' confidential information, the injury that Plaintiffs suffer to their business reputation compounds as consumers are likely to be left with the false perception that Plaintiffs cannot maintain the security of their own information. Such damage to Plaintiffs' business reputation is at least evidenced by comments of Plaintiffs actual

consumer, who indicated that they desired to get refunds for their purchases or otherwise discontinue Plaintiffs' services in light of the ongoing breach issue. Evans Decl. at ¶49.

Likewise, Plaintiffs' competitors are apparently trolling for specific competitive and confidential information (such as Plaintiffs' customer list), but, to Plaintiffs' knowledge, have not yet found them. *Id.* Loss of such customer list or market position cannot be recompensed by a monetary award, neither can injury to Mr. Evans' personal reputation. Plaintiffs simply cannot risk having its business, trade secrets and business reputation tarnished or destroyed by Defendants' illegal conduct, and thus this factor strongly supports entry of the requested relief. *Ruckelshaus v. Monsanto*, 463 U.S. 1315, 1317 (1983) (noting potential for irreparable harm if injunction was not in place where trade secrets could be used for the benefit of the trade secret holder's competitors).

III. THE BALANCE OF HARMS WEIGHS OVERWHELMINGLY IN PLAINTIFFS' FAVOR.

Any harm that Defendants may suffer if Plaintiffs' Motion is granted is nominal at best. Defendants have no right or legitimate reason to use, review or access The Confidential Information. To be clear, Plaintiffs do not seek to silence Defendants of their opinion or voice concerning Mr. Evans, Plaintiffs', or business practices. Plaintiffs are simply seeking to prevent Defendants from reviewing, accessing or otherwise using Plaintiffs' private, proprietary and confidential information and trade secrets.

Defendants simply have no right, interest or justifiable reason to have, for example, conversations and information relating to the medical testing of Mr. Evans' son, Plaintiffs' customer lists or the social security numbers of Plaintiffs' customers. Under Plaintiffs' Motion, Defendants are only restrained from violating the law. "Defendants cannot suffer compensable harm when enjoined from unlawful activity." *Specialty Chemicals & Serv.*, WL 618583 at *4.

On the other hand, as noted above, the harm to Plaintiffs if this Motion is denied is substantial and irreparable. For example, the Court must consider the considerable expense undertaken by Plaintiffs to invent, design, and develop its trade secrets (such as its source code and extensive customer list), the deliberate steps taken to ensure that its trade secrets remain confidential and the instantaneous loss in value Plaintiffs' trade secrets would incur if the Defendants were not enjoined from use or dissemination. Left unchecked, Defendants can review Plaintiffs' confidential and proprietary materials and do with it whatever they choose. Such a result is unwarranted, even where some of the information in the Confidential Information are not trade secrets, but are private and/or propriety. *Id.* at *6 (proprietary or confidential information, even if not trade secrets, may nevertheless be protected). Accordingly, the balance of hardships clearly weights in Plaintiffs' favor. *Id.*

IV. THE PUBLIC INTEREST WILL BE SERVED IF AN INJUNCTION IS GRANTED.

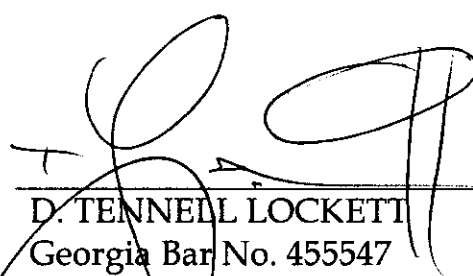
There is undoubtedly a strong public interest in protecting the privacy of members of the public and protecting companies' trade secrets, confidential and proprietary information, particularly, whereas here, Defendants have no reasonable or justifiable claim to such information. Moreover, Defendants' conduct, if sanctioned by this Court, would present a considerable policy concern inasmuch as it would effectively eviscerate any reasonable reliance on privacy, confidential or trade secret rights. Indeed, such a result would turn the Internet into a safe haven for computer hackers, disgruntled employees, those involved in corporate espionage or individuals working in concert therewith.

"[W]here court protection is based on bad faith and reprehensible business practices," the balancing of conflicting social and economic interests is particularly appropriate. *Cataphote Corp. v. Hudson*, 444 F.2d 1313, 1316 (5th Cir.1971). "[I]t is axiomatic that our laws protect private property and set standards for business competition and that obedience to such laws is in the public interest." *Continental Group, Inc. v. Amoco Chem. Corp.*, 614 F.2d 351, 357-58 (3d Cir.1980). The public is served by a strong discouragement of conduct such as Defendants' and accordingly this factor favors a grant of Plaintiffs' Motion.

CONCLUSION

For all of the foregoing reasons, Plaintiffs respectfully request that this Court grant is Motion for Temporary Restraining Order and Preliminary Injunctive Relief against Defendants as set forth more fully in the Motion filed concurrently herewith.

Respectfully submitted this 5TH day of February, 2011.



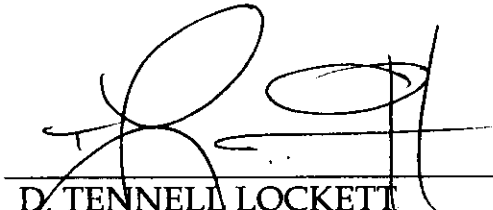
D. TENNELL LOCKETT
Georgia Bar No. 455547

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

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

LR 7.1.D., NDGa CERTIFICATION

The undersigned counsel for Plaintiffs state and certify that the foregoing brief has been prepared with one of the font and point selections approved by the court in LR 5.1B.



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

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