

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
Attorney for Plaintiff

IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT  
ST. CLAIR COUNTY, ILLINOIS  
LAW DIVISION

LIGHTSPEED MEDIA CORPORATION,

Plaintiff,

v.

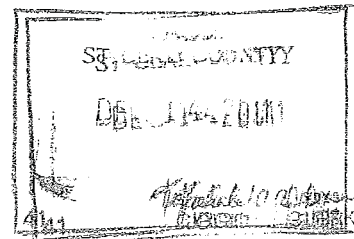
JOHN DOE,

Defendant.

No. L

Complaint

Jury Trial Demanded



Plaintiff, Lightspeed Media Corporation, through its undersigned counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as follows:

NATURE OF THE ACTION

1. Plaintiff files this action for computer fraud and abuse, conversion, unjust enrichment, breach of contract, and related civil conspiracy claim. Defendant and Defendant's co-conspirators, whose names Plaintiff expects to ascertain during discovery, used one or more hacked passwords to gain unauthorized access to Plaintiff's website and protected content and, upon information and belief continues to do the same. Plaintiff seeks a permanent injunction, statutory or actual damages, award of costs and attorneys' fees, and other relief.

THE PARTIES

2. Plaintiff is a corporation organized and existing under the laws of the State of Arizona, with its principal place of business located in Arizona.

3. Defendant's and his co-conspirators' actual names are unknown to Plaintiff. Instead, they are known to Plaintiff only by their Internet Protocol ("IP") addresses, which are numbers assigned to devices, such as computers, connected to the Internet. In the course monitoring website access, Plaintiff's agents observed unauthorized access of Plaintiff's

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

protected website through the IP addresses listed in on Exhibit A, attached hereto. Plaintiff believes that Defendant's identity will be revealed in discovery, at which time Plaintiff, if necessary, will seek leave of the Court to amend this Complaint to identify Defendant.

#### **JURISDICTION AND VENUE**

4. Pursuant to 735 ILCS 5/2-209, this Court has personal jurisdiction over Defendant because, upon information and belief, Defendant resides in or committed the unlawful acts in St. Clair County, Illinois. Plaintiff used geolocation technology to trace Defendant's location to St. Clair County. Although not a litmus test for personal jurisdiction, the use of geolocation gives Plaintiff good cause for asserting that personal jurisdiction is proper over Defendant.

5. Venue in this county is proper pursuant to 735 ILCS 5/2-101, because, upon information and belief, Defendant resides in St. Clair County, Illinois.

#### **POTENTIAL JOINDER OF CO-CONSPIRATORS**

6. Plaintiff may elect, after learning additional facts, to seek leave of the Court to amend this complaint to include Defendant's co-conspirators as defendants in this action pursuant to 735 ILCS 5/2-405.

#### **BACKGROUND**

7. The Internet has made nearly unlimited amounts of information and data readily available to anyone who wants to access it. Some of this information and data is private and available only to those who have lawful access to it. Owners attempt to protect this private content through the use of password authentication systems. Unfortunately, however, this does not ensure that content remains protected from unauthorized access.

8. Hacking is the act of gaining access without legal authorization to a computer or computer system. This is normally done through the use of special computer programming

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

software. This password cracking software repeatedly attempts to guess a password until the correct password is ascertained. The software can attempt a great number of passwords in a short period of time, sometimes even a million per second, making this type of software very efficient at obtaining a password. Individuals that utilize this type of software are called hackers.<sup>1</sup> Hackers employ various other means to gain unauthorized access to data such as identifying exploitable flaws in database codes.

9. Once a password is obtained, the hacker has unauthorized access to the protected content as long as the password remains valid. Sometimes a hacker will post the hacked password on a hacked password website, making it available to the members or visitors of that website. The hacker may even charge individuals for use of the hacked password and make a profit off of the loss and harm he or she has caused to the website owner or users. There are not necessarily any limits on how often or by how many people a password can be used, so a single hacked password can potentially allow unauthorized access to significant numbers of individuals.

### FACTUAL ALLEGATIONS

10. Plaintiff is the owner and operator of an adult entertainment website. Plaintiff invests significant capital in maintaining and operating this website. Plaintiff makes the website available only to those individuals who have been granted access to Plaintiff's website content (i.e. paying members). This access is given to members of the Plaintiff's website who sign-up and pay a fee to access the content. Access to this content is protected by a password assigned to each individual member.

---

<sup>1</sup> The technical definition of "hacker" is actually much broader and includes anyone who modifies a computer system to accomplish a goal—whether authorized or not (very similar to a computer programmer). A "cracker" is the technically correct definition of someone who gains unauthorized access to a computer. However, the common, popular definition of "hacking" is generally understood to be that of a "cracker." In this document any references to "hacker" or "hacking" will refer to their common definition of "cracker" or "cracking."

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

11. Defendant and Defendant's co-conspirators belong to a hacking community where hacked passwords are passed back and forth among the members. Members in this community work together to ensure that the members have access to normally inaccessible and unauthorized areas of the Internet. The series of transactions in this case involved accessing and sharing hacked passwords over the Internet and using the hacked passwords to access Plaintiff's website and private content. Defendant and his co-conspirators actively participated with one another in order to disseminate the hacked password, and intentionally engaged in a concerted action with one another to access the same website and content.

12. Defendant and his co-conspirators gained unauthorized access to Plaintiff's private website. They used hacked passwords to gain unlawful access to the member's sections of Plaintiff's websites. Through these hacked passwords Defendant and his co-conspirators consumed Plaintiff's content as though he or she was a paying member. They even downloaded Plaintiff's private content and disseminated that information to other unauthorized individuals.

13. Since Defendant and his co-conspirators accessed the website through hacked passwords, they are not required to provide any identifying personal information, such as their true names, addresses, telephone numbers or email addresses. Defendant and his co-conspirators can only be identified by their IP addresses.

14. Plaintiff retained Arcadia Data Security Consultants, LLC ("Arcadia") to identify IP addresses associated with hackers that use hacked passwords and the Internet to access Plaintiff's private website and content.

15. Arcadia used forensic software named Trader Hacker and Intruder Evidence Finder 2.0 (T.H.I.E.F.) to detect hacking, unauthorized access, and password sharing activity on

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

Plaintiff's websites. The individuals committing these unlawful activities are identified by their IP addresses as well as the dates and times they unlawfully accessed Plaintiff's websites.

16. Once Defendant's and his co-conspirators' IP addresses and dates and times of unlawful access were ascertained, Arcadia used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP addresses.

17. In addition to logging Defendant's IP addresses, Arcadia's software logged other important information into a uniform database, such as the specific websites that were unlawfully accessed and the files that were downloaded during that unauthorized access.

18. A summarization of the information gathered for Defendant is set forth in Exhibit A. The listing of the IP address, ISP, and date and time of the unauthorized access of Defendant's co-conspirators is set forth in Exhibit B. A declaration attesting to Arcadia's software is attached as Exhibit C.

#### COUNT I – COMPUTER FRAUD AND ABUSE

19. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

20. Defendant used one or more hacked passwords to gain unauthorized access to Plaintiff's website and protected content.

21. Once Defendant gained access, he downloaded Plaintiff's private content and disseminated that content to other unauthorized individuals.

22. Defendant's actions constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. A private right of action exists under the Act under 18 U.S.C. § 1030(g).

23. Defendant has caused loss to Plaintiff in the form of actual damages, statutory damages, and reputational injury, in excess of \$5,000.

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

24. The above alleged facts support claim of computer fraud and abuse by Plaintiff against Defendant.

### COUNT II – CONVERSION

25. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

26. Plaintiff has the exclusive right to the content contained in its protected websites, and is solely permitted to allow access to and disseminate that private content.

27. Plaintiff has an absolute and unconditional right to the immediate possession of the property as the owner of the websites as issue.

28. Defendant wrongfully, intentionally, and without authorization gained access to Plaintiff's protected website and downloaded Plaintiff's private content and disseminated that content to other unauthorized individuals. These actions are inconsistent with Plaintiff's right of possession.

29. Defendant knows, or has reason to know, that he does not have permission to access the private and password-protected areas of Plaintiff's website and that Plaintiff would demand the return of its protected content if it was aware of Defendant's identity.

### COUNT III – UNJUST ENRICHMENT

30. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

31. Defendant unjustly retained a benefit by accessing Plaintiff protected website and consuming and downloading Plaintiff's content without providing compensation for the services and content provided by Plaintiff.

Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

32. Defendant's benefit was to the Plaintiff's detriment as Plaintiff will not be compensated by Defendant or any other individual that was provided Plaintiff's content by Defendant. Additionally, Defendant's actions were to the Plaintiff's detriment by increasing Plaintiff's bandwidth costs and causing Plaintiff reputational harm.

33. Defendant continues to benefit from the unjust benefit of Plaintiff's protected content and this violates the fundamental principles of justice, equity, and good conscience.

#### **COUNT IV – BREACH OF CONTRACT**

34. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

35. To lawfully access Plaintiff's website, users must state that they agree with the following statement: "I have come to this website knowing it's [sic] contents and agree to view sexually explicit material for my personal use. Viewing such material does not knowingly violate the community standards of the area in which I live."

36. Defendant violated this user agreement by using the material on Plaintiff's protected website for more than just personal use by disseminating the material to other unauthorized individuals.

37. Defendant also violated this user agreement by knowingly violating the community standard where he lives, because Defendant's violations of the law are presumably a violation of the community standards.

#### **COUNT V – CIVIL CONSPIRACY**

38. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.



Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

39. Defendant and his co-conspirators engaged in a concerted action to share hacked passwords amongst each other that would allow entry into Plaintiff's protected website.

40. Defendant and his co-conspirators used those hacked passwords to gain unauthorized access to Plaintiff's website.

41. Once Defendant and his co-conspirators gained access to Plaintiff website, they downloaded protected content from that website and shared that content amongst themselves and with other unauthorized individuals.

42. As a proximate result of this conspiracy, Plaintiff has been damaged, as is more fully alleged above.

#### **JURY DEMAND**

43. Plaintiff hereby demands a jury trial in this case.

#### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff respectfully requests Judgment and relief as follows:

1) Judgment against Defendant that he has: a) committed computer fraud and abuse against Plaintiff pursuant to 18 U.S.C. § 1030(g); b) converted Plaintiff's protected content; c) become unjustly enriched at the expense of Plaintiff; d) breached the contractual agreement he had with Plaintiff; and e) Defendant conspired with other individuals to committed the above unlawful activities;

2) Judgment in favor of the Plaintiff against the Defendants for actual damages or statutory damages pursuant to 18 U.S.C. § 1030(g) and common law, at the election of Plaintiff, in an amount in excess of \$100,000 to be ascertained at trial;



Michael O'Malley, Esq.  
Carey, Danis, & Lowe  
*Attorney for Plaintiff*

3) Order of impoundment under 17 U.S.C. §§ 503 & 509(a) impounding all copies of Plaintiff's audiovisual works, photographs or other materials, which are in Defendant's possession or under his control;

4) On Count V, an order that Defendant is jointly and severally liable to the Plaintiff in the full amount of the Judgment on the basis of a common law claim for civil conspiracy; for an award of compensatory damages in favor of the Plaintiff and against Defendant, jointly and severally, in an amount to be determined at trial;

5) Judgment in favor of Plaintiff against the Defendants awarding the Plaintiff attorneys' fees, litigation expenses (including fees and costs of expert witnesses), and other costs of this action; and


6) Judgment in favor of the Plaintiff against the Defendants, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted under the circumstances.

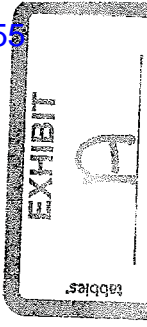
Respectfully submitted,

LIGHTSPEED MEDIA CORPORATION

DATED: December 12, 2011

By:

  
Michael O'Malley, Esq. (Bar No. 3125757)  
Carey, Danis, & Lowe  
5111 W. Main Street  
Bellville, Illinois 62226  
(618) 212-6300  
MO'Malley@careydanis.com  
*Attorney for Plaintiff*



IP Address	Date/Time (UTC)	Internet Service Provider	Websites Accessed	Files Downloaded
75.132.153.113	11/28/2011 16:24	Charter Communications	<a href="http://www.angelwoods.com">www.angelwoods.com</a> <a href="http://www.dirtyaly.com">www.dirtyaly.com</a> <a href="http://www.ericafightspeed.com">www.ericafightspeed.com</a> <a href="http://www.lightsspeedteemetwork.com">www.lightsspeedteemetwork.com</a> <a href="http://www.lightsspeedtv.com">www.lightsspeedtv.com</a> <a href="http://www.sweetdevon.com">www.sweetdevon.com</a>	/members/content/vids/agl_0001_sunblock1/lsc_ltv_15454-full.wmv /members/content/JOR/L2/lsc-jor-16325-063.jpg /members/content/JOR/L2/lsc-jor-16325-105.jpg /members/content/solo/blue_bed/lsc-aw-15420-064.jpg /members/content/solo/blue_bed/lsc-aw-15420-102.jpg 27 more files not listed