

Received  
07/07/12  
N 1408

July 2, 2012

STATE OF ILLINOIS  
IN THE CIRCUIT COURT OF THE THIRD JUDICIAL CIRCUIT  
MADISON COUNTY  
(618) 296-4464  
WWW.CO.MADISON.IL.US

CASE No. 2012 L 000927

DATE: July 02, 2012

LIGHTSPEED MEDIA CORPORATION

PLAINTIFF

VS.

LUCAS SHASHEK

DEFENDANT

DEFENDANT: LUCAS SHASHEK

You are hereby summoned and required to file an answer in this case, or otherwise file your appearance, in the office of the Madison County Circuit Clerk, within 30 days after service of this summons, exclusive of the day of service. If you fail to do so, a judgment or decree by default may be taken against you for the relief prayed in the complaint.

This summons must be returned by the officer or other person to whom it was given for service, with endorsement thereon of service and fees, if any, immediately after service. If service cannot be made, this summons shall be returned so endorsed.

This summons may not be served later than 30 days after its date.

Witness: JUDY NELSON the Clerk of said Circuit Court and the seal thereof, at Edwardsville, Illinois, this July 2, 2012 .

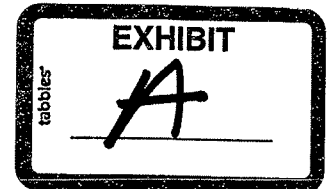


JUDY NELSON  
CLERK OF THE CIRCUIT COURT

BY: W Bentlage  
Deputy Clerk

(Plaintiff's attorney or plaintiff if he is not represented by an attorney)  
PAUL DUFFY  
PRENDA LAW INC  
161 N CLARK ST STE 3200  
CHICAGO IL 60601

Date of Service: \_\_\_\_\_, 20\_\_\_\_.  
(To be inserted by officer on the copy left with the defendant or other person)



**FILED**

JUL 02 2012

CLERK OF CIRCUIT COURT #6  
THIRD JUDICIAL CIRCUIT  
MADISON COUNTY, ILLINOIS

IN THE CIRCUIT COURT OF THE THIRD JUDICIAL CIRCUIT  
MADISON COUNTY, ILLINOIS  
LAW DIVISION

LIGHTSPEED MEDIA CORPORATION,

Plaintiff,

v.

LUCAS SHASHEK,

Defendant.

No.

122927

Complaint

Jury Trial Demanded

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

**NATURE OF THE ACTION**

1. Plaintiff LIGHTSPEED MEDIA CORPORATION ("Plaintiff") files this action for computer fraud and abuse, conversion, unjust enrichment, breach of contract, and negligence. Defendant LUCAS SHASHEK ("Defendant") used one or more hacked username/passwords to gain unauthorized access to Plaintiff's Internet website and protected content and, upon information and belief, continues to do the same. Plaintiff seeks a permanent injunction, statutory damages 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 is an individual adult over the age of eighteen whom, upon information and belief, is currently, and at all relevant times mentioned herein, a resident of the County of Madison.

#### JURISDICTION AND VENUE

4. Pursuant to 735 ILCS 5/2-209, this Court has personal jurisdiction over Defendant because Defendant resides in or committed the unlawful acts in Madison County, Illinois.

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

#### BACKGROUND

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

7. 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 software that "cracks" the password. 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 information exploitable flaws in database codes.

---

<sup>1</sup> The technical definition of a "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, and be indistinguishable from, the common definitions of "cracker" or "cracking."

8. 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 username/password on a hacked username/password website, making it available to the members or visitors of that website. The posting hacker may even charge individuals for use of the hacked username/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 username/password can potentially allow unauthorized access to significant numbers of individuals.

#### FACTUAL ALLEGATIONS

9. Plaintiff is the owner and operator of an adult entertainment website. Plaintiff invests significant capital in maintaining and operating its 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 Plaintiff's owned content. Access to this content is protected by a password assigned to each individual member.

10. Further, to prevent access to those who are not members of Plaintiff's website, Plaintiff employs the services of Proxigence, and its ProxyPass security system. ProxyPass, according to the Proxigence website, "is an Apache module that defends websites against members-area attacks and violations... [and] customers rely on ProxyPass to prevent the theft of protected content..." (See <http://www.proxigence.com/pp-about.html>, last checked on June 4, 2012.) On information and belief, ProxyPass constitutes the industry standard for Internet security password protection.

11. On information and belief, security systems such as ProxyPass are not infallible, and can be successfully bypassed through the efforts of savvy hackers, allowing such hackers to view the content that a client, like Plaintiff, attempts to protect.

12. On information and belief, Defendant belongs to a hacking community where hacked username/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 username/passwords over the Internet and using the hacked username/passwords to access Plaintiff's website and private content. Defendant participated with other hackers in this community in order to disseminate the hacked username/password, and intentionally acted to access Plaintiff's website and content through a hacked username/password.

13. Defendant gained unauthorized access to Plaintiff's private website. He used hacked username/passwords to gain unlawful access to the member's sections of Plaintiff's websites. Through these hacked username/passwords Defendant consumed Plaintiff's content as though he was a paying member. Further, he downloaded Plaintiff's private content and disseminated that information to other unauthorized individuals.

14. Since Defendant accessed the website through a hacked username/password(s), he would not have been required to provide any identifying personal information, such as his or her true name, address, telephone number or email address.

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

16. 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 Plaintiff's websites.

17. In addition to logging Defendant's IP address, 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. Once Defendant's IP address 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 identified by Arcadia as those used to perpetrate the hacking.

19. Through a separate case arising in a different state, Plaintiff sought, and received, a court order demanding that the various ISPs who issued the hacking IP addresses divulge the identifying personal information of those account holders associated with those IP addresses.

20. Through this prior suit, Plaintiff was able to discover that Defendant's IP address 24.207.181.55—was one of the hacking IP addresses identified by Arcadia through the process described above.

21. On information and belief, Defendant was assigned IP address 24.207.181.55 from Charter and was in control of it during all relevant times, including, but not limited to, on September 25, 2011 at 03:33:00 (UTC), which was the date and time that Defendant hacked Plaintiff's website and content per Arcadia's observations.

#### COUNT I – COMPUTER FRAUD AND ABUSE

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

23. On or around September 25, 2011 at 03:33:00 (UTC), Defendant, using IP address 24.207.181.55, used a specific private hacked username/password ("hacked username/password") to knowingly, and with intent to defraud, gain unauthorized access to Plaintiff's password-protected website and protected computer content described above.

24. Defendant's use of a hacked username/password to gain access to Plaintiff's private content was based on an actual and/or implicit misrepresentation by Defendant that this hacked username/password actually authorized Defendant to access Plaintiff's website and content.

25. Defendant's use of a hacked username/password to gain this access, however, was clearly not authorized by Plaintiff.

26. Defendant's actions, as well as his identity, while using the hacked username/password were concealed from Plaintiff by the manner described above.

27. Once Defendant gained this access, on information and belief, he downloaded Plaintiff's private content and purposefully disseminated that content to other unauthorized individuals.

28. 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).

29. Defendant has caused loss to Plaintiff in the form of actual damages, statutory damages, and reputational injury, in excess of \$5,000. Plaintiff suffered damage through Defendant accessing, without authorization, Plaintiff's website and downloading for free Plaintiff's content, and passing this content onto others. Normally, in the absence of this violation, Plaintiff would charge a fee to Defendant, as well as the others, to access this privately owned content. Defendant's hacking and redistributing not only substantially devalued

Plaintiff's work in and of itself, but also gave hundreds, if not thousands, of other individuals the ability to access such private content for no charge. As such, Plaintiff sustained damages through the prevention of these sales, and devaluation of Plaintiff's content.

#### COUNT II – CONVERSION

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

31. In doing the acts and deeds herein ascribed to him, Defendant appropriated and converted access to Plaintiff's member's only website to his own use and benefit in express violation of duties and obligations owed to Plaintiff.

32. Plaintiff has the exclusive property interest in access to the content contained on its members-only websites, and is solely permitted to allow access to and disseminate that private content.

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

34. Defendant wrongfully, intentionally, and without authorization gained access to Plaintiff's protected website and disseminated that access information to other unauthorized individuals. These actions are inconsistent with Plaintiff's right of possession and resulted in wrongful deprivation of Plaintiff's property interest in its exclusive contents.

35. 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.

36. As a direct and proximate result of the forgoing, Plaintiff sustained damage in an amount to be determined at trial, together with interest thereon.

///



**COUNT III – UNJUST ENRICHMENT**

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

38. Defendant knowingly and unjustly received benefit and value by unlawfully accessing Plaintiff's members-only website and consuming and downloading Plaintiff's content without providing compensation for the services and content provided by Plaintiff.

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

40. Defendant continues to benefit from the unjust benefit of Plaintiff's protected content without paying fair value for it and this violates the fundamental principles of justice, equity, and good conscience.

**COUNT IV – BREACH OF CONTRACT**

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

42. 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." In return for this attestation, Plaintiff allows individuals to access its website and its Internet content.

43. Plaintiff, after receiving this agreement, allowed Defendant to access its website and content under the false pretenses that Defendant was in fact a paying consumer, and not using a hacked username/password to access the site.

44. Defendant viewed the above statement, agreed to it, but failed to perform his obligations under the agreement.

45. Defendant violated and breached 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.

46. Defendant also violated and breached 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.

47. As a direct and proximate result of such a breach, Plaintiff sustained extensive, and currently incalculable, damage, to be determined at trial, together with interest thereon.

#### COUNT V – NEGLIGENCE

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

49. In the alternative, Defendant accessed, or controlled access to, the Internet connection used in performing the unauthorized hacking of Plaintiff's exclusive content, proximately causing financial harm to Plaintiff.

50. In the alternative, on information and belief, Defendant had a duty to secure his Internet connection. Defendant breached that duty by failing to secure his Internet connection.

51. Reasonable Internet users take steps to secure their Internet access accounts preventing the use of such accounts for an illegal purpose. Defendant's failure to secure his

Internet access account, thereby allowing for its illegal use, constitutes a breach of the ordinary care that a reasonable Internet account holder would do under like circumstances.

52. In the alternative, Defendant secured his connection, but permitted an unknown third party to use his Internet connection to hack into, and disseminate, Plaintiff's content. Defendant knew, or should have known, that this unidentified individual used Defendant's Internet connection for the aforementioned illegal activities. Defendant declined to monitor the unidentified third-party hacker's use of his computer Internet connection, demonstrating further negligence.

53. In the alternative, Defendant knew of, and allowed for, the unidentified third party infringer's use of his Internet connection for illegal purposes and thus was complicit in the unidentified third party's actions.

54. Upon information and belief, Plaintiff alleges that Defendant's failure to secure his Internet access account directly allowed for the hacking and sharing of Plaintiff's content through Defendant's Internet connection, and interfered with Plaintiff's exclusive rights and privacy in Plaintiff's exclusive content, which, from there, was shared with numerous others.

55. Upon information and belief, Plaintiff alleges that Defendant knew, or should have known of, the unidentified third party's infringing actions, and, despite this, Defendant directly, or indirectly, allowed for the hacking Plaintiff's website and content through Defendant's Internet connection, and interfered with Plaintiff's exclusive rights.

56. By virtue of his unsecured access, Defendant negligently allowed the use of his Internet access account to perform the above-described unlawful actions that caused direct harm to Plaintiff.

57. Had Defendant taken reasonable care in securing access to this Internet connection, or monitoring the unidentified third-party individual's use of his Internet connection, such hacking as those described above would not have occurred by the use of Defendant's Internet access account.

58. Defendant's actions allow others to unlawfully copy and share Plaintiff's private website content, proximately causing financial harm to Plaintiff and unlawfully interfering with Plaintiff's exclusive rights.

#### JURY DEMAND

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

#### PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays judgment and relief against defendant 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, alternatively, e) Defendant was negligent in his allowance of this hacking to occur via his Internet access connection;
- 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;
- 3) Order of impoundment under 17 U.S.C. §§ 503 & 509(u) impounding all copies of Plaintiff's audiovisual works, photographs or other materials, which are in Defendant's possession or under his control;

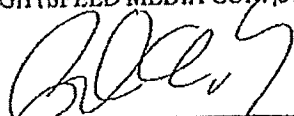
- 4) Judgment in favor of Plaintiff against the Defendants awarding the Plaintiff attorneys' fees, litigation expenses (including fees and costs of expert witnesses), and other costs of this action; and
- 5) Judgment in favor of the Plaintiff against Defendant, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted under the circumstances.

Respectfully submitted,

LIGHTSPEED MEDIA CORPORATION

DATED: June 27, 2012

By:

  
Paul Duffy, Esq. (Bar No. 6210496)  
Prenda Law Inc.  
161 N. Clark St. Suite 3200  
Chicago, IL 60601  
Telephone: (312) 880-9160  
Facsimile: (312) 893-5677  
E-mail: paduffy@wofightpiracy.com

*Attorney for Plaintiff*

July 2, 2012

IN THE CIRCUIT COURT  
FOR THE THIRD JUDICIAL CIRCUIT  
MADISON COUNTY, ILLINOIS

CASE NUMBER: 2012 L 000927

LIGHTSPEED MEDIA CORPORATION

Plaintiff(s)

VS.

LUCAS SHASHEK

Defendant(s)

**FILED**

JUL 02 2012

CLERK OF CIRCUIT COURT #6  
THIRD JUDICIAL CIRCUIT  
MADISON COUNTY, ILLINOIS

ASSIGNMENT ORDER

The above case is hereby assigned to the Honorable ANN CALLIS for setting and disposition.

Clerk to send copies of this Order to the attorneys of record and any pro se party.

DATE: July 02, 2012

s/Ann Callis  
Chief Judge