

MICHAEL K. JEANES
Clerk of the Superior Court
By Ruth Bartlett, Deputy
Date 05/25/2012 Time 1:48pm
Description Amount
----- CASE# CV2012-053194 -----
CIVIL NEW COMPLAINT 301.00

TOTAL AMOUNT 301.00
Receipt# 22210211

1 Steven James Goodhue (#029288)
Law Offices of Steven James Goodhue
2 9375 East Shea Blvd., Suite 100
Scottsdale, AZ 85260
3 Telephone: (480) 214-9500
Facsimile: (480) 214-9501
4 E-Mail: sjg@sjgoodlaw.com

5 *Attorney for Plaintiff*
Lightspeed Media Corporation

7 **IN THE SUPERIOR COURT FOR THE STATE OF ARIZONA**
8 **IN AND FOR THE COUNTY OF MARICOPA**

9
10 LIGHTSPEED MEDIA CORPORATION, an
Arizona corporation,
11 Plaintiff,
12 v.
13 ADAM SEKORA,
14 Defendant.

CV2012-053194
CV2012-
COMPLAINT AND JURY DEMAND
(I) COMPUTER FRAUD;
(II) CONVERSION;
(III) UNJUST ENRICHMENT;
(IV) BREACH OF CONTRACT; AND
(V) NEGLIGENCE

(Assigned to the Hon. _____)

16 Plaintiff, LIGHTSPEED MEDIA CORPORATION, by and through its undersigned
17 counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as
18 follows:

19 **NATURE OF THE ACTION**

20 1. Plaintiff LIGHTSPEED MEDIA CORPORATION ("Plaintiff") files this action
21 for computer fraud and abuse, conversion, unjust enrichment, breach of contract, and negligence.
22 Defendant Adam Sekora ("Defendant") used one or more username/hacked passwords to gain
23 unauthorized access to Plaintiff's Internet website and protected content and, upon information
24

1 and belief, continues to do the same. Plaintiff seeks a permanent injunction, statutory damages
2 or actual damages, award of costs and attorneys' fees, and other relief.

3 **THE PARTIES**

4 2. Plaintiff is a corporation organized and existing under the laws of the State of
5 Arizona, with its principle place of business located in Arizona. Plaintiff is and was at all times
6 mentioned herein qualified to do business in Arizona.

7 3. Defendant is an individual adult over the age of eighteen whom, upon information
8 and belief, is currently, and at all relevant times mentioned herein, a resident of the County of
9 Maricopa.

10 **JURISDICTION AND VENUE**

11 4. Pursuant to Art 6, § 14 of the Arizona Constitution, this Court has original subject
12 matter jurisdiction in this case because this is a civil action over the amount of \$5,000.

13 5. Jurisdiction is proper in the Superior Court of the State of Arizona generally
14 because, on information and belief, Defendant was domiciled in the State, and/or committed the
15 alleged unlawful actions within the State.

16 6. Venue is proper in the County of Maricopa pursuant to A.R.S. § 12-401 *et al.*
17 because, on information and belief, Defendant was domiciled in the County, and/or committed
18 the alleged unlawful actions within the County.

19 **BACKGROUND**

20 7. The Internet has made nearly unlimited amounts of information and data readily
21 available to anyone who desires access to it. Some of this information and data is private,
22 available only to those who have a lawful access to it. Owners' attempts to protect this private
23 content through the use of password authentication systems. Unfortunately, this safety device
24 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 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.¹ Hackers employ various other means to gain unauthorized access to data such as identifying information 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 username/hacked password on a username/hacked password website, making it available to the members or visitors of that website. The posting hacker may even charge individuals for use of the username/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 username/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 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

¹ 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.”

1 and pay a fee to access Plaintiff's owned content. Access to this content is protected by a
2 password assigned to each individual member.

3 11. Further, to prevent access to those who are not members of Plaintiff's website,
4 Plaintiff employs the services of Proxigence, and its ProxyPass security system. ProxyPass,
5 according to the Proxigence website, "is an Apache module that defends websites against
6 members-area attacks and violations... [and] customers rely on ProxyPass to prevent the theft of
7 protected content..." (See <http://www.proxigence.com/pp-about.html>, last checked on May 19,
8 2012.) On information and belief, ProxyPass constitutes the industry standard for Internet
9 security password protection.

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

13 13. On information and belief, Defendant belongs to a hacking community where
14 username/hacked passwords are passed back and forth among the members. Members in this
15 community work together to ensure that the members have access to normally inaccessible and
16 unauthorized areas of the Internet. The series of transactions in this case involved accessing and
17 sharing username/hacked passwords over the Internet and using the username/hacked passwords
18 to access Plaintiff's website and private content. Defendant participated with other hackers in
19 this community in order to disseminate the username/hacked password, and intentionally acted to
20 access Plaintiff's website and content through a username/hacked password.

21 14. Defendant gained unauthorized access to Plaintiff's private website. He used
22 username/hacked passwords to gain unlawful access to the member's sections of Plaintiff's
23 websites. Through these username/hacked passwords Defendant consumed Plaintiff's content as
24

1 though he was a paying member. Further, he downloaded Plaintiff's private content and
2 disseminated that information to other unauthorized individuals.

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

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

9 17. Arcadia used forensic software named Trader Hacker and Intruder Evidence
10 Finder 2.0 (T.H.I.E.F.) to detect hacking, unauthorized access, and password sharing activity on
11 Plaintiff's websites.

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

15 19. Once Defendant's IP address and dates and times of unlawful access were
16 ascertained, Arcadia used publicly available reverse-lookup databases on the Internet to
17 determine what Internet Service Provider ("ISP") issued the IP addresses identified by Arcadia
18 as those used to perpetrate the hacking.

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

22 21. Through this prior suit, Plaintiff was able to discover that Defendant's IP address
23 174.138.169.218 was one of the hacking IP addresses identified by Arcadia through the process
24 described above.

22. On information and belief, Defendant was assigned IP address 174.138.169.218 from an ISP called "Secured Servers" and was in control of it during all relevant times, including, but not limited to, on December 5, 2011 at 16:58:00 UTC, which was the date and time that Defendant hacked Plaintiff's website and content per Arcadia's observations.

FIRST CLAIM FOR RELIEF

COMPUTER FRAUD AND ABUSE

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

24. On or around December 5, 2011 at 16:58:00 UTC, Defendant, using IP address, 174.138.169.218, used a specific username/hacked password ("Username/Hacked Password") to knowingly, and with intent to defraud, gain unauthorized access to Plaintiff's password-protected website and protected computer content described above.

25. Defendant's use of a Username/Hacked Password to gain access to Plaintiff's private content was based on an actual and/or implicit misrepresentation by Defendant that this Username/Hacked Password actually authorized Defendant to access Plaintiff's website and content.

26. Defendant's use of a Username/Hacked Password to gain this access, however, was clearly not authorized by Plaintiff.

27. Defendant's actions, as well as his identity, while using the Username/Hacked Password were concealed from Plaintiff by the manner described above.

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

1 29. Defendant's actions constitute a violation of the Computer Fraud and Abuse Act,
2 18 U.S.C. § 1030. A private right of action exists under the Act under 18 U.S.C. § 1030(g).

3 30. Defendant has caused loss to Plaintiff in the form of actual damages, statutory
4 damages, and reputational injury, in excess of \$5,000. Plaintiff suffered damage through
5 Defendant accessing, without authorization, Plaintiff's website and downloading for free
6 Plaintiff's content, and passing this content onto others. Normally, in the absence of this
7 violation, Plaintiff would charge a fee to Defendant, as well as the others, to access this privately
8 owned content. Defendant's hacking and redistributing not only substantially devalued
9 Plaintiff's work in and of itself, but also gave hundreds, if not thousands, of other individuals the
10 ability to access such private content for no charge. As such, Plaintiff sustained damages
11 through the prevention of these sales, and devaluation of Plaintiff's content.

12 **SECOND CLAIM FOR RELIEF**

13 **CONVERSION**

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

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

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

22 34. Plaintiff has an absolute and unconditional right to the immediate possession of
23 the property as the owner of the websites as issue.
24

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

5 36. Defendant knows, or has reason to know, that he does not have permission to
6 access the private and password-protected areas of Plaintiff's website.

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

9 **THIRD CLAIM FOR RELIEF**

10 **UNJUST ENRICHMENT**

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

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

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

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

1 **FIFTH CLAIM FOR RELIEF**

2 **NEGLIGENCE**

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

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

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

10 52. Reasonable Internet users take steps to secure their Internet access accounts
11 preventing the use of such accounts for an illegal purpose. Defendant's failure to secure his
12 Internet access account, thereby allowing for its illegal use, constitutes a breach of the ordinary
13 care that a reasonable Internet account holder would do under like circumstances.

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

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

23 55. Upon information and belief, Plaintiff alleges that Defendant's failure to secure
24 his Internet access account directly allowed for the hacking and sharing of Plaintiff's content

1 through Defendant's Internet connection, and interfered with Plaintiff's exclusive rights and
2 privacy in Plaintiff's exclusive content, which, from there, was shared with numerous others.

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

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

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

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

17 **JURY DEMAND**

18 60. Plaintiff hereby demands a jury trial in this case.

19 **PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiff respectfully prays judgment and relief against defendant as
21 follows:

22 a. Judgment against Defendant that he has: a) committed computer fraud and abuse
23 against Plaintiff pursuant to 18 U.S.C. § 1030(g); b) converted Plaintiff's protected content; c)
24 become unjustly enriched at the expense of Plaintiff; d) breached the contractual agreement he

1 had with Plaintiff; and, alternatively, e) Defendant was negligent in his allowance of this hacking
2 to occur via his Internet access connection;

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


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

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

12 f. Judgment in favor of the Plaintiff against Defendant, awarding Plaintiff
13 declaratory and injunctive or other equitable relief as may be just and warranted under the
14 circumstances.

15 Dated this 24th day of May, 2012
16

17 Law Offices of Steven James Goodhue

18 By: 
19 Steven James Goodhue (#029288)
20 9375 East Shea Blvd., Suite 100
Scottsdale, AZ 85260

21 *Attorney for Plaintiff,*
22 *Lightspeed Media Corporation*
23
24