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

LIGHTSPEED MEDIA CORPORATION,

Plaintiff,

v.

ANTHONY SMITH, SBC INTERNET SERVICES, INC., d/b/a AT&T INTERNET SERVICES, AT&T CORPORATE REPRESENTATIVE #1, COMCAST CABLE COMMUNICATIONS, LLC and COMCAST CORPORATE REPRESENTATIVE #1,

Defendants.

Case No. 11-L-683

Jury Trial Demanded

FIRST AMENDED COMPLAINT

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

NATURE OF THE ACTION

1. Plaintiff files this action against Defendant Anthony Smith for computer fraud and abuse, conversion, unjust enrichment, breach of contract, and related civil conspiracy claims. Defendant and Defendant's co-conspirators, whose names Plaintiff has repeatedly sought to ascertain during discovery, used one or more hacked passwords to gain unauthorized access to Plaintiff's websites and protected computer 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.

2. Plaintiff files this action against Defendants AT&T and Comcast (collectively, the "ISPs"), and/or a corporate representative of each entity, for negligence, computer fraud and abuse, civil conspiracy, violations of the Illinois Consumer Fraud and Deceptive Practices Act

and aiding and abetting. These ISPs, directly and through their respective corporate representatives, have, among other things, allowed their respective subscribers to repeatedly and persistently hack into and steal from Plaintiff's website; and, upon information and belief, failed to take reasonable action to prevent their subscribers from hacking into and stealing from Plaintiff's website; failed to warn their subscribers to cease and desist in such conduct; interfered with Plaintiff's efforts to identify and take action to prevent the subscribers' illegal and tortious activity; and, through a direct policy decisions, inaction or for other reasons, allowed the continued and pervasive criminal and tortious acts by certain of their subscribers against Plaintiff.

THE PARTIES

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

4. Defendant Anthony Smith's 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 of monitoring website access, Plaintiff's agents observed unauthorized access of Plaintiff's protected websites through the IP addresses listed on the Exhibits attached to the original Complaint.

5. Defendant SBC Internet Services, Inc. is a corporation organized and existing under the laws of the State of California, with its principal place of business in Dallas, Texas. AT&T is an internet service provider ("ISP") that has, among other things, knowingly assisted, or negligently allowed, Defendant Smith's co-conspirators to engage in the widespread, persistent and continuing hacking into Plaintiff's protected website, and to misappropriate and

disseminate content from Plaintiff's website. AT&T has opposed and interfered with all of Plaintiff's attempts to ascertain the identities of AT&T's subscribers who are involved in this widespread criminal activity, prevented Plaintiff from any available mechanism for obtaining damages and stopping the hacking, and acted as the *de facto* legal counsel for Defendant Smith's co-conspirators by asserting substantive claims and defenses to liability on their behalf in litigation here and throughout the Nation. AT&T has thus allowed the extensive criminal activity to continue, and it has profited, and continues to profit, from the illegal activity of the conspiracy, by continuing to seek monthly subscription fees from members of the conspiracy while sheltering and assisting continued civil and criminal wrongdoing.

6. AT&T Corporate Representative 1 is the individual who, upon information and belief, is a director, officer or employee of AT&T with authority to direct AT&T to fail or refuse to comply with valid subpoenas served upon to AT&T seeking the identities of Defendant Smith's co-conspirators; to fail or refuse to prevent AT&T's subscribers from continued hacking of, and theft from, Plaintiff; to authorize AT&T to act as the *de facto* legal counsel to allow its subscribers to continue theft from Plaintiff; and to authorize AT&T's decision to fail or refuse to perform activities that would inhibit its subscribers from committing tortious and criminal acts against Plaintiff.

7. Defendant Comcast Cable Communications, LLC. ("Comcast") is a limited liability company organized and existing under the laws of the State of Delaware, with its principal place of business in Philadelphia, Pennsylvania. Comcast is an ISP that has, among other things, knowingly assisted, or negligently allowed, Defendant Smith's co-conspirators to engage in the widespread, persistent and continuing hacking into Plaintiff's protected website. Comcast has opposed and interfered with Plaintiff's attempts to ascertain the identities of

Comcast's customers who are involved in this widespread criminal activity, prevented Plaintiff from seeking damages and stopping the hacking into its website, and acted as the *de facto* legal counsel for members of the conspiracy by asserting substantive claims and defenses to liability on their behalf in litigation here and throughout the Nation. Comcast has thus allowed the extensive theft to continue, and it has profited, and continues to profit, from the illegal activity of the conspiracy, by continuing to seek monthly subscription fees from members of the conspiracy while sheltering and assisting continued civil and criminal wrongdoing.

8. Comcast Corporate Representative 1 is the individual who, upon information and belief, is a director, officer or employee of Comcast with authority to direct Comcast to fail or refuse to comply with valid subpoenas served upon to Comcast seeking the identity of Defendant Smith and his co-conspirators; to fail or refuse to prevent Comcast's subscribers from continued hacking of, and theft from, Plaintiff; to authorize Comcast to act as the *de facto* legal counsel to allow its subscribers to continue theft from Plaintiff; to authorize Comcast's decision to fail or refuse to comply with such subpoenas; and to authorize Comcast to take actions to limit its subscribers' criminal and civil wrongdoing.

JURISDICTION AND VENUE

9. Pursuant to 735 ILCS 5/2-209, this Court has personal jurisdiction over Defendant Smith because, upon information and belief, Defendant Smith resides in or committed the unlawful acts in St. Clair County, Illinois.

10. This Court has personal jurisdiction over the other Defendants because each has participated in, or allowed, the commission of unlawful acts in St. Clair County, Illinois. This Court also has personal jurisdiction over the remaining Defendants under the doctrines of pendent and supplemental jurisdiction.

11. Venue in this county is proper pursuant to 735 ILCS 5/2-101, because, upon information and belief, Defendant Smith resides in St. Clair County, Illinois, and the actions giving rise to the causes of action alleged herein occurred, in whole or in part, in St. Clair County, Illinois.

POTENTIAL JOINDER OF CO-CONSPIRATORS

12. 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

13. 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.

14. 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. 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]

[1] 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."

Hackers employ various other means to gain unauthorized access to data such as identifying exploitable flaws in database codes.

15. 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 REGARDING DEFENDANT SMITH AND HIS CO-CONSPIRATORS

16. Plaintiff is the owner and operator of adult entertainment websites. Plaintiff invests significant capital in maintaining and operating those websites. Plaintiff makes the websites 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 websites 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.

17. Defendant Smith and Defendant Smith'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 Plaintiff's secured websites. The series of transactions in this case involved accessing, agreeing to share, sharing hacked passwords over the Internet and using the hacked passwords to access Plaintiff's protected websites and private computer content. Defendant Smith and his co-conspirators actively participated with one another in order to

disseminate the hacked passwords, and intentionally engaged in a concerted action with one another to access the same websites and content.

18. Defendant Smith and his co-conspirators gained unauthorized access to Plaintiff's protected websites. They used hacked passwords to intentionally gain unauthorized access to the member's sections of Plaintiff's protected websites. Through these hacked passwords Defendant Smith and his co-conspirators consumed Plaintiff's content as though they were paying members. They downloaded Plaintiff's private computer content and disseminated that information to other unauthorized individuals.

19. Since Defendant Smith and his co-conspirators accessed Plaintiff's protected websites through hacked passwords, they were 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.

20. 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 protected websites and private computer content.

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

22. Once Defendant Smith 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.

23. In addition to logging Defendant Smith'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.

24. Defendant was detected by the T.H.I.E.F. Security System gaining unauthorized access to Plaintiff's protected websites on November 24, 2011 at 01:09 (UTC). This date was the latest time the T.H.I.E.F. Security System detected Defendant's unauthorized access.

25. Defendant was detected by the T.H.I.E.F. Security System accessing, without authorization, ten (10) of the Plaintiff's protected websites. Further, Defendant was detected downloading more than seventy-two (72) private computer files from these websites.

26. A listing of the IP address, ISP, and date and time of one of unauthorized accesses of Defendant Smith and his co-conspirators is set forth in an Exhibit to the original Complaint. A declaration attesting to Arcadia's software is attached as an Exhibit to the original Complaint, a signed copy of which is on file with the Court in this matter.

FACTUAL ALLEGATIONS AGAINST ISPs AND THEIR CORPORATE REPRESENTATIVES

27. AT&T has never contested or disputed allegations that certain of its subscribers have hacked into, and stolen from, Plaintiff's website.

28. Comcast has never contested or disputed allegations that certain of its subscribers have hacked into, and stolen from, Plaintiff's website.

29. At the outset of this litigation, the ISPs and their Representatives were simply third-party custodians who were the sole holders of identifying information of their subscribers who have been hacking into and stealing from Plaintiff's website. Plaintiff attempted, through the only means available to it, to obtain that identifying information through discovery.

30. The ISPs, upon information and belief, through the approval and authorization of the Corporate Representative of each entity, chose to interpose themselves in this litigation, interfere with the Court's Orders, evade subpoenas, and prevent and obstruct Plaintiff from learning the identities of those ISP subscribers hacking into and stealing from its website. Further, upon information and belief, the ISPs have not taken any actions to prevent their subscribers from committing criminal and tortious acts against Plaintiff even after being on actual notice of the criminal and tortious activity and having full control over the Internet accounts of their subscribers.

31. A significant percentage of the alleged criminal and tortious actors are AT&T or Comcast subscribers. As such, the delay tactics and other interference on the part of the ISPs has prevented Plaintiff from learning the identities of a vast number of Defendant Smith's co-conspirators.

32. Plaintiff requested, and this Court on or about December 16, 2011 granted, leave to serve discovery in order to learn the identities of Defendant Smith and his co-conspirators.

33. In accordance with that Court Order, Plaintiff served subpoenas upon all of the internet service providers listed in Paragraph A of the Court Order, including AT&T and Comcast.

34. Upon being served with the subpoenas, the ISPs sought to delay and derail this litigation, thereby shielding their subscribers from liability and allowing them to continue their unfettered hacking and theft from Plaintiff's website.

35. ISPs ran interference for their paying customers, despite allegations certain of those customers were using their subscriptions to commit criminal acts.

36. The ISPs have not provided the identity of hackers who are also their subscribers to Plaintiff.

37. The ISPs instead filed several motions to extend the time in which to respond to the subpoenas.

38. The ISPs, rather than responding, moved to quash the subpoenas. The Court, after hearing extensive evidence and argument from the ISPs, entered orders on April 27 and May 21, 2012, in which it directed the ISPs, among other things, to produce subscriber information for the Court to review *in camera* before disclosing it to Plaintiff.

39. Rather than comply with that order, the ISPs caused further delay by filing a petition with the Illinois Supreme Court under Supreme Court Rule 383, seeking a supervisory order to preclude the disclosure of subscriber information to the Court for *in camera* review. The Illinois Supreme Court on June 24, 2012 granted that petition and vacated the May 24, 2012 order.

40. In seeking to quash the subpoenas, and in submitting the Rule 383 Petition, the ISPs made numerous arguments for which it had no standing, on behalf of its subscribers who have been identified as hackers.

41. The ISPs, among other things, challenged on grounds only available to parties to litigation, such as lack of personal jurisdiction, improper joinder, challenges to the sufficiency of factual allegations in the Complaint under 735 ILCS 5/2-615, and other arguments that are available only to litigants to make.

42. The ISPs also argued that the burden on their subscribers of producing identifying information in response to subpoenas served upon them was excessive. The ISPs made this

argument despite the fact that the subpoenas imposed no burden on the subscribers because the ISPs, and not subscribers, were the only ones required to take action.

43. The ISPs chose to act as if they were parties to this litigation, and have obstructed any attempt by Plaintiff to stop the hacking into, and theft from, its website.

44. Every action that the ISPs have taken in connection with this litigation has served to delay litigation and to prevent Plaintiff from preventing hacking. Every action that the ISPs have taken in connection with this litigation has prevented Plaintiff from asserting its rights, preventing criminal activity against it, or obtaining any relief for harm caused to it.

45. The ISPs did not and have not produced evidence suggesting that they have notified any of their subscribers to cease and desist the illegal hacking into, and theft from, Plaintiff's website.

46. The ISPs did not and have not produced evidence suggesting that they have cancelled a single contract with a subscriber on the ground that Plaintiff has identified it as having stolen from its website.

47. The ISPs did not and have not produced evidence suggesting that they have notified law enforcement officials that certain of their subscribers have engaged in criminal activity against Plaintiff.

48. Upon information and belief, the ISPs have taken no reasonable action to prevent the massive level of hacking into, and theft from, Plaintiff's website, which continues to this day.

49. The ISPs and their respective Corporate Representatives have thus enabled and sheltered the continued massive hacking into and theft from Plaintiff's website.

50. The extent of the hacking that the ISPs continue to enable is demonstrated by the fact that between August 1 and December 6, 2011 alone, Plaintiff's software blocked well over 330,000 unauthorized sign-on attempts to its website (over 2,500 per day).

51. The IP addresses listed in the Complaint represent less than two percent (2%) of the attempts to hack into Plaintiff's website. In total, hackers illegally downloaded over 170,000 files, using more than 3.5 terbytes of total bandwith, from Plaintiff's website.

52. Furthermore, upon information and belief, nearly twenty percent, or 1,805, of the group of subscribers that the ISPs seek to protect have attempted to hack into Plaintiff's website with a new, hacked user- or passcode, since this litigation began. This amount continues to increase daily. Of those, at least seventy-five have each attempted to hack Plaintiff's website five or more times each since this action began.

COUNT I – COMPUTER FRAUD AND ABUSE
(All Defendants)

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

54. Defendant Smith intentionally used one or more hacked passwords to gain unauthorized access to Plaintiff's protected websites and protected computer content.

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

56. Defendants AT&T and Comcast, with the approval of the respective Corporate Representatives, failed and refused to take action to prevent hacking into, and theft from, Plaintiff's website.

57. As a result of Defendants' actions, or failure to take appropriate actions, Plaintiff had to take remedial actions in order to prevent the rampant and ongoing unauthorized access to

its protected websites and private computer content. Plaintiff retained Arcadia to identify Defendant Smith and other hackers that were gaining unauthorized access to Plaintiff's protected websites, so Plaintiff could this remedial legal action and prevent any further unauthorized access. The cost to Plaintiff for Arcadia to create the T.H.I.E.F. Security System to identify Defendant and other hackers was in excess of $250,000.

58. The cost to Plaintiff for Arcadia to host and run the T.H.I.E.F. Security System is $500.00 per month. The T.H.I.E.F. Security System was used by Arcadia to detect the hacking and unauthorized access of Plaintiff's websites for eleven (11) months, from August of 2011 to July of 2012. The total cost to host and use the T.H.I.E.F. Security System for those eleven (11) months was $5,500.00.

59. The minimum cost to gain lawful, authorized access to Plaintiff's websites is $39.95 for a single month of membership. The average membership to Plaintiff's website lasts 2 months. Members of the conspiracy have damaged Plaintiff in the amount of $519,350 in lost revenues by gaining, or allowing and failing to prevent, unauthorized access to Plaintiff's protected websites instead of authorized access.

60. Defendants have thus damaged Plaintiff in the amount of at least $774,850 in economic damages for the remedial measures Plaintiff was forced to take to prevent further unauthorized access to its websites by Defendant Smith and other hackers.

61. Defendants' 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).

COUNT II – CONVERSION
(Defendant Smith)

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

63. 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.

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

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

66. Defendant Smith knows, or has reason to know, that he does not have permission to access the private and password-protected areas of Plaintiff's websites and Plaintiff has demanded the return of its protected content from Defendant Smith.

67. The above alleged facts support a claim of conversion by Plaintiff against Defendant Smith.

COUNT III – UNJUST ENRICHMENT
(Defendant Smith)

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

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

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

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

72. The above alleged facts support a claim of unjust enrichment by Plaintiff against Defendant Smith.

COUNT IV – UNJUST ENRICHMENT
(Defendants AT&T and Comcast)

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

74. Defendant ISPs unjustly retained a benefit by failing to take action to prevent their subscribers who participated in the conspiracy from illegally accessing Plaintiff's protected website, and consuming and downloading Plaintiff's content, without providing compensation for the services and content provided by Plaintiff. The subscriber fees that Defendant ISPs collected from Defendant Smith and/or his co-conspirators included, in part, fees from those who illegally used the Internet to commit criminal and tortious acts against Plaintiff.

75. Defendant ISPs were also unjustly enriched because, while engaging in a dilatory legal strategy designed solely to prevent Plaintiff from learning the identities of their subscribers, they, upon information and belief, continued to collect subscriber fees from subscribers who did, and continued to, hack into and steal from Plaintiff's website.

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

77. Defendants continue to benefit from the unjust benefit of Plaintiff's protected content and this violates the fundamental principles of justice, equity, and good conscience.

78. The above alleged facts support a claim of unjust enrichment by Plaintiff against Defendants.

COUNT V – BREACH OF CONTRACT
(Defendant Smith)

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

80. To lawfully access Plaintiff's websites, 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."

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

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

83. The above alleged facts support a claim of breach of contract by Plaintiff against Defendant.

COUNT VI – CIVIL CONSPIRACY
(Defendant Smith and Smith's Co-Conspirators)

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

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

86. Defendant Smith and his co-conspirators, by sharing hacked passwords among themselves that were created solely for the purpose of illegally gaining access to Plaintiff's website, reached an agreement to hack into and steal from Plaintiff's website.

87. Defendant and his co-conspirators used those hacked passwords to gain unauthorized access to Plaintiff's protected websites.

88. Once Defendant and his co-conspirators gained access to Plaintiff's websites, they downloaded protected content from those websites and shared that content amongst themselves and with other unauthorized individuals.

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

COUNT VII – CIVIL CONSPIRACY
(Defendants Smith, AT&T, AT&T's Corporate Representative, Comcast and Comcast's Corporate Representative)

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

91. Defendant Smith and his co-conspirators hacked into and stole from Plaintiff's website.

92. Defendants AT&T and Comcast were informed, at a minimum through Plaintiff's initial complaint in this matter, that certain of their subscribers were hacking into and stealing from Plaintiff's website.

93. Upon information and belief, Defendants AT&T and Comcast have failed to take action sufficient to prevent their subscribers from hacking into and stealing from Plaintiff's website.

94. Instead, AT&T and Comcast, previously nonparties to this litigation, instead chose to act as *de facto* legal counsel for Defendant Smith and his co-conspirators by asserting substantive defenses to liability that only a party to litigation, and not third-party information repositories, may assert, all in an effort to obstruct Plaintiff from learning who stole from it.

95. To the extent that AT&T and Comcast acted as *de facto* legal counsel for Defendant Smith's co-conspirators, in exchange for continued receipt of subscriber fees from Defendant Smith's co-conspirators, the Defendants reached an agreement to allow and/or shelter the continued hacking into an theft from Plaintiff's website as a component of the services provided in exchange for subscriber fees.

96. The Corporate Representative of each of AT&T and Comcast who elected to allow their subscribers to continue their unrestrained criminal and tortious activity against Plaintiff, to the extent they facilitated and allowed criminal activity against Plaintiff to continue. The Corporate Representative of AT&T and Comcast, therefore, is each personally liable for involvement in civil conspiracy.

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

COUNT VIII – ILLINOIS CONSUMER FRAUD AND DECEPTIVE PRACTICES ACT
(Defendants AT&T and Comcast)

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

99. Defendant Smith's, and his co-conspirators', use of a hacked passwords to illegally gain entry into and steal from Plaintiff's website is a deceptive practice.

100. Defendant AT&T's and Comcast's efforts to defend those gaining illegal access to Plaintiff's website from being identified, while at the same time failing to prevent the individuals from continued unlawful entry into the website, is a deceptive practice.

101. The Defendants intended the Plaintiff to rely upon their deceptive practices because, among other things, their conduct allowed Defendant Smith's co-conspirators to re-gain unauthorized entry into Plaintiff's website under the false guise that they were legitimate, paying customers. Defendants' deception occurred in the course of conduct involving trade.

102. Plaintiff was actually damaged by Defendants' deception in the form of, among other things, lost revenues from the theft and distribution of its conduct without payment.

103. Defendants AT&T and Comcast are therefore liable to Plaintiff for damages pursuant to the Illinois Consumer Fraud and Deceptive Business Practices Act ("Act"), 815 ILCS 505/1, *et seq*.

COUNT X – AIDING AND ABETTING
(Defendants AT&T, AT&T Corporate Representative, Comcast, Comcast Corporate Representative)

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

105. At all times relevant hereto, Defendants AT&T and Comcast, and their corporate representatives, knew or should have known that certain of their subscribers were accused of hacking into and stealing from Plaintiff's website.

106. Defendants AT&T and Comcast aided and abetted Defendant Smith and his co-conspirators in the illegal hacking and theft from Plaintiff by, among other things, failing to take

action to prevent such conduct, and acting as *de facto* legal counsel for Smith and his co-conspirators in an effort to prevent Plaintiff from learning of their identities, aided and abetted the hacking into, and theft from, Plaintiff's website.

107. Furthermore, to the extent that the actions of AT&T and Comcast in those respects allowed and enabled criminal activity to occur and/or continue against Plaintiff, the decisions of the Corporate Representative for each entity who was responsible for those actions were not within their scope of employment. As such, each Corporate Representative is personally liable to Plaintiff for aiding and abetting the hacking into, and theft from, Plaintiff's website.

108. Furthermore, the actions of AT&T and Comcast, and each respective Corporate Representative, in those regards were willful, malicious, intentional, aggravated, and were committed with reckless and/or deliberate disregard of an unjustifiable and substantial risk of significant harm to Plaintiff, and as such, Plaintiff should be entitled to punitive damages from Defendants AT&T and Comcast and their respective Corporate Representative.

JURY DEMAND

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests Judgment and relief as follows:

1) With respect to Count I, judgment against Defendants that they have: a) committed or allowed computer fraud and abuse against Plaintiff pursuant to 18 U.S.C. § 1030(g); and b) converted, or allowed conversion of, Plaintiff's protected content;

2) With respect to Count II, judgment that Defendant Smith has converted property belonging to Plaintiff;

3) With respect to Count III, judgment that Defendant Smith has become unjustly enriched at the expense of Plaintiff;

4) With respect to Count IV, judgment that Defendant Comcast and AT&T have become unjustly enriched at the expense of Plaintiff;

5) With respect to Count V, judgment that Defendant Smith breached the contractual agreement he had with Plaintiff;

6) With respect to Count VI, judgment that Defendant Smith conspired with other individuals to commit the unlawful activities set forth herein;

7) With respect to Count VII, judgment that all Defendants conspired among each other, and with others, to commit the unlawful activities set forth herein;

8) With respect to Count VIII, judgment that Defendants AT&T and Comcast are therefore liable to Plaintiff for damages pursuant to the Illinois Consumer Fraud and Deceptive Business Practices Act ("Act"), 815 ILCS 505/1, *et seq.*;

9) With respect to Count IX, judgment that Defendants AT&T and Comcast, and the Corporate Representative of each entity, aided and abetted commission of the unlawful activities set forth herein;

10) 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 $200,000 to be ascertained at trial;

11) Judgment in favor of the Plaintiff, and against AT&T and Comcast and their respective Corporate Representatives for punitive damages;

12) 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 Smith's possession or under his control;

13) An order that Defendants are 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 Defendants, jointly and severally, in an amount to be determined at trial;

14) 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

15) 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: August 3, 2012

By: /s/ Kevin T. Hoerner

Kevin T. Hoerner (Bar No. 06196686)
Becker, Paulson, Hoerner & Thompson P.C.
5111 W. Main Street
Bellville, Illinois 62226
(618) 235-0020
Counsel for Plaintiff

Paul Duffy (Bar No. 06210496)
Prenda Law, Inc.
161 N. Clark Street, Suite 3200
Chicago, IL 60601
Telephone: (312) 880-9160
Facsimile: (312) 893-5677
E-mail: paduffy@wefightpiracy.com
Counsel for Plaintiff