IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

GUAVA, LLC,

Plaintiff,

v.

Does 1-5,

Defendants.

CASE NO. 12-cv-8000

Judge:

Magistrate Judge:

COMPLAINT

JURY TRIAL DEMANDED

Plaintiff GUAVA, LLC ("Plaintiff"), by and through its undersigned counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as follows

NATURE OF THE CASE

1. Plaintiff files this action for computer fraud and abuse, civil conspiracy, conversion and negligence arising from unlawful computer-based breaches and data distribution. By this action, Guava seeks, *inter alia*, compensatory damages, injunctive relief and attorney's fees and costs.

PARTIES

2. Plaintiff is a limited liability company that operates protected computer systems, including computer systems accessible throughout Illinois.

3. Defendants' actual names are unknown to Plaintiff. Instead, Defendants are known to Plaintiff only by individual Internet Protocol addresses ("IP addresses"), each of which is a number assigned to devices, such as computers, that are connected to the Internet. In the course of monitoring individuals seeking unauthorized access to Plaintiff's websites, Plaintiff's agents observed unlawful reproduction and distribution occurring over the five IP addresses

listed in Exhibit A hereto. Plaintiff cannot ascertain Defendants' actual identities without limited expedited discovery.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to the Federal Computer Fraud and Abuse Act, codified at 18 U.S.C. §§ 1030, *et seq.*, (the "CFAA"), and pursuant 28 U.S.C. § 1331 (actions arising under the laws of the United States). This Court has supplemental jurisdiction over the conspiracy, conversion and negligence claims because they are so related to Plaintiff's CFAA claim, which is within this Court's original jurisdiction, that the claims form part of the same case and controversy under Article III of the United States Constitution.

5. This Court has personal jurisdiction over the Defendants because, upon information and belief, they either reside in or committed copyright infringement within the State of Illinois. Plaintiff used geolocation technology to trace the IP addresses of each Defendant to a point of origin within the State of Illinois. This Court has personal jurisdiction over non-resident Defendants, if any, under the Illinois long-arm statute, 735 ILCS 5/2-209(a)(2), because they each used one or more hacked usernames/passwords to gain unauthorized access to Plaintiff's Internet website and take protected systems, thus committing tortious acts within the meaning of the statute, and because they participated in a civil conspiracy to hack into and steal from Plaintiff's websites with Illinois residents.

6. Venue is properly founded in this Court pursuant to 28 U.S.C. §§ 1391(b) and 1400(a) because Defendants reside in this District, may be found in this District, or a substantial part of the events giving rise to the claims in this action occurred within this District.

7. Joinder of Defendants is proper because all Defendants participated in the same civil conspiracy to commit to gain unauthorized access to Plaintiff's websites.

BACKGROUND

8. 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 attempt to protect this private information through the use of password authentication systems. Unfortunately, this safety device does not ensure that information remains protected from unauthorized access.

9. 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.

10. Once a password is obtained, the hacker has unauthorized access to the protected information 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 that he or she has caused to the website owner or users. There are not necessarily any limits on how often or by how many

[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."

people a password can be used, so a single hacked username/password can potentially allow unauthorized access to significant numbers of individuals.

FACTUAL ALLEGATIONS

11. Plaintiff is the owner and operator protected computer systems, including protected computer systems that are accessible in Illinois.

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

13. Plaintiff's computer systems are regularly targeted by hackers who wish to gain unauthorized access to Plaintiff's valuable information.

14. When hackers successfully breach Plaintiff's protected systems, they and their fellow co-conspirators take, and may distribute, the misappropriated information in a highly-coordinated manner to their fellow Internet-based co-conspirators.

15. The process of probing Plaintiff's defenses, breaching Plaintiff's protected systems and distributing misappropriated information is an ongoing problem that continues to this day.

16. On information and belief, security systems to prevent hacking are not infallible, and can be successfully bypassed through the efforts of savvy hackers, allowing such hackers to access the systems that a client, like Plaintiff, attempts to protect.

17. On information and belief, each Defendant belongs to a hacking community where hacked usernames/passwords are passed back and forth among members. Members of

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 systems. Defendants participated with each other, and with other hackers in this community, in order to disseminate the hacked usernames/passwords, and intentionally acted to access Plaintiff's website and systems through the use of hacked usernames/passwords.

18. Defendants gained unauthorized access to Plaintiff's private websites. They used hacked usernames/passwords to gain unlawful access to the member's sections of Plaintiff's websites. Through these hacked usernames/passwords each Defendant accessed Plaintiff's systems as though they were paying members. Further, they downloaded Plaintiff's private information, which is not available to members, and disseminated that information to other unauthorized individuals.

19. Since Defendants accessed the website through hacked usernames/passwords, they would not have been required to provide any identifying personal information, such as his or her true name, address, telephone number or email address.

20. Plaintiff retained a forensic computer consultant to identify IP addresses associated with hackers who use hacked usernames/passwords and the Internet to access Plaintiff's private websites and systems.

21. The forensic evidence gathered on behalf of Plaintiff identified that the IP addresses attached at Exhibit A were used for hacking, unauthorized access, and/or password sharing activity on Plaintiff's websites.

22. In addition to logging Defendants' IP addresses, Plaintiff obtained other important information, such as the specific websites that were unlawfully accessed and the files that were downloaded during that unauthorized access.

23. Once Defendants' IP addresses and dates and times of unlawful access were ascertained, Plaintiff used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP addresses and the putative location of those IP addresses used to perpetrate the hacking.

24. On information and belief, each Defendant was assigned a corresponding IP addresses listed in Exhibit A hereto. Furthermore, on information and belief, each Defendant was in control of the corresponding IP address during all relevant times.

COUNT I – COMPUTER FRAUD AND ABUSE

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

26. Defendants, each using his or her using IP address as listed in Exhibit A, used specific private hacked usernames/passwords ("hacked usernames/passwords") to knowingly, and with intent to defraud, gain unauthorized access to Plaintiff's password-protected website and protected computer systems described above.

27. Defendants' use of hacked usernames/passwords to gain access to Plaintiff's private systems was based on an actual and/or implicit misrepresentation by each Defendant that the hacked usernames/passwords actually authorized the Defendant to access Plaintiff's website and private systems.

28. Defendants' use of hacked usernames/passwords to gain that access, however, was clearly not authorized by Plaintiff.

29. Defendants' actions, as well as their identities, while using hacked usernames/passwords were concealed from Plaintiff in the manner described above.

30. Once each Defendant gained this access, on information and belief, he or she accessed Plaintiff's private systems and purposefully took information, and/or shared it with unauthorized individuals. Those systems contained, among other things, information regarding the identities of Plaintiff's customers; account information; financial information and/or computer programming or security information; and other information that Plaintiff protects and to which it does not give third parties access, even those who pay for and obtain legitimate passwords to access Plaintiff's websites.

31. Those actions on the part of each Defendant constitute violations 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).

32. Defendants have caused loss to Plaintiff during a one-year period in excess of $5,000, including fees paid to its computer forensics agents, fees paid to legal counsel, fees paid to secure its systems, fees paid to investigators, bandwidth fees, and other costs.

33. Plaintiff has suffered damage due to the foregoing actions. Normally, in the absence of those actions, Plaintiff would charge a fee to Defendants, as well as the others, to access its privately-owned systems. Defendants, by hacking and taking information from those systems, not only substantially devalued Plaintiff's services, it also gave to hundreds, if not thousands, of other individuals the ability to access such private systems for no charge. As such, Plaintiff sustained damages through the prevention of these sales, and devaluation of the value of its websites.

COUNT II – CIVIL CONSPIRACY

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

35. Each of the Defendants used hacked usernames/passwords to gain access to Plaintiff's private systems. That access was based on an actual and/or implicit misrepresentation by each Defendant that the hacked username/password actually authorized the Defendant to access Plaintiff's websites and systems.

36. Each Defendant, upon information and belief, belongs to a hacking community whose members share hacked usernames/passwords among other members. Members of this work together to ensure that the members have access to normally inaccessible and unauthorized areas of the Internet.

37. By using and sharing hacked passwords/usernames, each Defendant acted in concert with other members of this hacking community, and in a concerted action with other members, to accomplish unlawful transfers of Plaintiff's protected information.

38. Each time a Defendant used a shared and hacked password/username, he or she reached an agreement with another co-conspirator(s) within the hacking community whereby the member provided the username/password in order to allow the Defendant to unlawfully access and obtain protected information from Plaintiff's websites.

39. Each Defendant had express or constructive knowledge that, in accomplishing the purposes of their common agreement, they were not acting unilaterally, and it was not fortuitous or accidental that the Defendants performed acts in agreement with others for the purpose of misappropriating Plaintiff's protected systems.

40. Each Defendant understood the general objectives of the conspiratorial scheme, accepted them, and agreed, either explicitly or implicitly to do its part to further those objectives.

41. In furtherance of this civil conspiracy, Defendants committed overt tortious and unlawful acts by using hacked usernames/passwords to impermissibly obtain access to, and misappropriate private information from, Plaintiff's websites.

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

COUNT III – CONVERSION

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

44. In committing the acts and deeds herein ascribed to him or her, each Defendant appropriated and converted access to Plaintiff's members-only website, and its private information, to his or own use and benefit, in express violation of duties and obligations owed to Plaintiff.

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

46. Plaintiff has an absolute and unconditional right to the immediate possession of the property as the owner of the websites and private information at issue.

47. Each 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 systems.

48. Each Defendant, through the act of accessing Plaintiff's private systems and removing information, converted that information to a tangible form.

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

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

COUNT IV – NEGLIENCE

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

52. Each Defendant accessed, or controlled access to, the Internet connection used in performing the unauthorized hacking of Plaintiff's exclusive and protected information, proximately causing financial harm to Plaintiff.

53. In the alternative, on information and belief, each Defendant had a duty to secure his or her Internet connection, and each breached that duty by failing to secure his or her Internet connection and allowing a third-party to use that connection. It was reasonably foreseeable that, if the Defendant failed to secure his or her Internet connection, a third-party could use the connection to hack into Plaintiff's websites and removed protected information from it.

54. Reasonable Internet users take steps to secure their Internet access accounts preventing the use of such accounts for an illegal purpose. Each Defendant's failure to secure his or her Internet access account, thereby allowing for its illegal use, constitutes a breach of the ordinary care that a reasonable Internet account holder would observe under like circumstances.

55. In the alternative, each Defendant secured his or her connection, but permitted an unknown third party to use his Internet connection to hack into, and disseminate, Plaintiff's

private information. Each Defendant knew, or should have known, that this unidentified individual used Defendant's Internet connection for the aforementioned illegal activities. Each Defendant declined to monitor the unidentified third-party hacker's use of his or her computer Internet connection, demonstrating further negligence.

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

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

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

59. By virtue of his or her failure to secure access to his or her Internet connection, each Defendant negligently allowed the use of Internet access account to perform the above-described unlawful actions that caused direct harm to Plaintiff.

60. Had each Defendant taken reasonable care in securing access to this Internet connection, or monitoring the unidentified third-party individual's use of his or her Internet

connection, such hacking as those described above would not have occurred by the use of the Defendant's Internet access account.

61. Each Defendant's actions allowed others to unlawfully copy and share access to Plaintiff's private website and protected information, proximately causing financial harm to Plaintiff and unlawfully interfering with Plaintiff's exclusive rights.

JURY DEMAND

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays judgment and relief against each Defendant as follows:

1) Judgment against each Defendant that he or she has: a) committed computer fraud and abuse against Plaintiff pursuant to 18 U.S.C. § 1030(g); b) converted Plaintiff's protected information; c) become unjustly enriched at the expense of Plaintiff; d) breached the contractual agreement he had with Plaintiff; and, alternatively, e) that each 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(a) impounding all copies of Plaintiff's audiovisual works, photographs or other materials, which are in any 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 Defendants, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted.

Respectfully submitted,

Guava LLC

DATED: October 5, 2012

By: /s/ Paul Duffy

Paul A. Duffy, Esq. (Bar NO. 6210496)
Prenda Law, Inc.
161 N. Clark St., Suite 3200
Chicago, IL 60601
Phone: 312-880-9160
Fax: 312-893-25677
E-mail: paduffy@wefightpiracy.com
Attorney for Plaintiff

EXHIBIT A