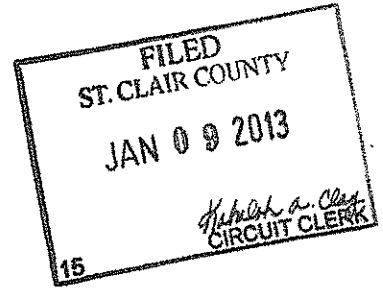


IN THE CIRCUIT COURT OF  
THE TWENTIETH JUDICIAL CIRCUIT  
ST. CLAIR COUNTY, ILLINOIS



LW SYSTEMS, LLC,

Plaintiff,

v.

CHRISTOPHER HUBBARD,

Defendant.

Case No. 13-L-

15

**COMPLAINT AT LAW**

Plaintiff LW Systems, LLC, by and through its attorneys, for its Complaint against Defendant, states and alleges as follows.

**Introduction**

Defendant has unlawfully used and damaged Plaintiff's computers for his personal financial gain, while willfully disregarding Plaintiff's right to use and enjoy its personal property. Defendant deceptively gained unauthorized access to and installed software on Plaintiff's computers that allowed others to gain unauthorized access to those computers. The functioning of Plaintiff's computers was materially impaired as a result of this unauthorized access. Plaintiff brings this action to enjoin Defendant's unlawful misconduct and seek compensation for the damage he and his co-conspirators caused.

**Parties**

1. Plaintiff LW Systems, LLC is a limited liability company that operates a nationwide business in matching adult content copyright holders with adult website operators. Plaintiff does not own copyrights itself, but instead operates a computer service that is marketed

to website operators who are seeking copyrighted content for their sites. Plaintiff's computers manage the logistics of matching website operators with content and then delivering that content.

2. Defendant Christopher Hubbard is a resident of the State of Illinois.

### **Jurisdiction and Venue**

3. This Court has personal jurisdiction over Defendant because, *inter alia*, Defendant resides in Illinois.

4. Venue is proper in this Court because the transactions complained of herein occurred in St. Clair County, Illinois.

### **Factual Allegations Common to All Counts**

5. Plaintiff operates a computer service that allows adult website operators to supplement their existing content libraries, in whole or in part, with content produced by third-parties. Plaintiff does not own the copyrights in this content, but instead owns and operates computers that host and deliver the content. The services offered by Plaintiff range from supplementing a website's existing content library to providing a turn-key website content solution.

6. A core concern for computer service operators, such as Plaintiff, is computer security. Plaintiff's computers are its key business assets. They allow website operators to review available third-party content and to finalize their content transactions. Without properly functioning computers, Plaintiff's business cannot function.

7. Computer security is a serious issue for any business that operates computers. *See* Michael Mimoso, *Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks*, THE THREAT POST, Oct. 4, 2012 (explaining that "[a]s many as 30 banks have been targeted" recently by cyber hackers.); Bryon Acohido, *No Slowdown in Sight for*

*Cyberattacks*, USA TODAY, July 30, 2012 (Eddie Schwartz, chief security officer of security firm RSA stating that “[i]t’s easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy.”).

8. Neither large corporations nor governments are immune from computer security issues. *See* Kim Zetter, *Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop*, WIRED, Sept. 4, 2012 (explaining that a hacker group obtained “1 million Apple device IDs that” were “obtained from an FBI computer they hacked.”).

9. The courts have an important role to play in discouraging computer misuse. *See* Glenn Chapman, *Cyber Defenders Urges to go on the Offense*, AMERICAN FREE PRESS, July 26, 2012 (former FBI cyber crime unit chief Shawn Henry explaining that “I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction.” and Black Hat founder Jeff Moss proposing that “cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.”).

10. Plaintiff’s computers are secured by user authentication systems. Individuals seeking to legitimately access Plaintiff’s computers must possess valid username and password credentials. These credentials are not publicly available. Nor are they marketed or distributed to consumers. Instead, they are provided to website operators who wish to browse the content that is available for license from third-party copyright holders.

11. Defendant belongs to a community of individuals who have agreed to assist one another in gaining unauthorized access to computers and then share with one another the information stored on those systems. Defendant and his co-conspirators combined and agreed with one another to collaborate in gaining unauthorized access to Plaintiff’s computers and to

distribute the information stored on Plaintiff's computers amongst one another. Specifically, on information and belief Defendant and his co-conspirators shared information about vulnerabilities in Plaintiff's computer systems, encouraged one another on Internet chat rooms to proceed with breaching Plaintiff's computers, and then collaborated to distribute the information they secured from Plaintiff's computers.

12. Plaintiff did not provide Defendants or any of his co-conspirators with credentials to its computer or access to the content thereon.

13. Defendant intentionally installed software on Plaintiff's computers that allowed him and others to access Plaintiff's computers without Plaintiff's permission and against Plaintiff's will. The software installed on Plaintiff's computers is referred to as "Malware." As used herein, "Malware" describes computer software installed on an end-user's computer over the Internet to record to facilitate unauthorized access to a computer.

14. For example, a computer infected with Malware would transmit a report of activity on a computer, such as keystrokes, and would allow a third-party to access the computer without permission.

15. Malware can be installed onto a computer in several different ways. On information and belief, Defendant and his co-conspirators utilized one or more of the following methods to install unauthorized software on Plaintiff's computers.

- a. First, Malware can be installed by someone who gains unauthorized physical access to computer systems. In these circumstances a third-party can

bypass startup authentication systems via use of a boot disk<sup>1</sup> and install software on a computer.

b. Second, Malware can be installed remotely by someone who uses social engineering to target individuals with administrative access to a computer. By way of example, someone could send a computer administrator an e-mail with a file attachment or link that purports to come from a reliable source. When the attachment is opened or the file is viewed, code is executed that results in Malware installation.

c. Third, Malware can be installed remotely by someone who takes advantage of a known unpatched software security hole. Security flaws associated with Windows-based systems and other software, such as PDF documents, are regularly reported and exist until software vendors release an update patch that closes the security hole.

16. Once Malware is installed, the installing person can gain unauthorized access to a computer. On information and belief, Defendant and his co-conspirators installed Malware onto Plaintiff's computers, used the Malware to generate false credentials to Plaintiff's systems and otherwise bypass Plaintiff's authentication systems, overwhelmed Plaintiff's systems with unlawful usage and activity, and distributed the information contained on Plaintiff's computers to others and amongst themselves.

17. Defendant's Malware destroyed and rendered functionless Plaintiff's authentication systems. Furthermore, Defendant's Malware caused Plaintiff's computers to slow down, used up memory on Plaintiff's computer and frustrated Plaintiff's ability to use its

---

<sup>1</sup> One example of a boot disk that allows someone with unauthorized physical access to bypass Windows startup authentication systems is Knoppix.

computers to operate its business. Furthermore, Plaintiff was forced to keep its computers running longer (due to the slowed performance) which utilizes more electricity and decreases the useful life of a computer. Furthermore, Plaintiff was forced to incur costs and expenses associated with removing the Malware and guarding against future Malware attacks. Finally, Plaintiff suffered significant reputational harm from the breach of its computers.

18. Plaintiff retained a forensic computer consultant to identify IP addresses associated with Defendant and his co-conspirators.

19. Once Defendant's IP address 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 address and the putative location of the IP address used to perpetrate the hacking.

**Count I**  
**Trespass to Personal Property/Chattels**

20. Plaintiff re-alleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

21. At all times relevant hereto, Plaintiff owned and was in possession of the computer or internet connection that was infected by Defendant's software.

22. Defendant and his co-conspirators intentionally and without consent, used Plaintiff's computer and internet connections, gained access to Plaintiff's computers, accessed various components and systems within Plaintiff's computers, obtained access to information about Plaintiff and its computers, burdened the processors, hard drives and other components of Plaintiff's computers, and dispossessed Plaintiff of access to its computers.

23. In so doing, Defendant and his co-conspirators intentionally intermeddled and interfered with, damaged, and deprived Plaintiff to its computer and/or Internet connection, or a portion thereof.

**Count II**  
**Nuisance**

24. Plaintiff re-alleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

25. Defendant and his co-conspirators intentionally and without consent, used Plaintiff's computer and internet connections, gained access to Plaintiff's computers, accessed various components and systems within Plaintiff's computers, obtained access to information about Plaintiff and its computers, burdened the processors, hard drives and other components of Plaintiff's computers, and dispossessed Plaintiff of access to its computers.

26. In so doing, Defendant and his co-conspirators intentionally and substantially invaded and interfered with Plaintiff's interest and enjoyment in its computer systems.

**Count III**  
**Negligence**

27. Plaintiff re-alleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

28. Defendant and his co-conspirators, having gained access to Plaintiff's computers, had a duty not to harm the computers and impact their operation.

29. Defendant and his co-conspirators breached this duty by damaging Plaintiff's computers and interfering with their operation.

30. As a direct and proximate result of Defendant's negligence and that of his co-conspirators, Plaintiff was damaged and harmed as alleged herein.

**Count IV**  
**Computer Tampering**

31. Plaintiff re-alleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

32. Defendant and his co-conspirators knowingly and without authorization of Plaintiff inserted the computer software program, Malware, into Plaintiff's computer systems.

33. The computer software program, Malware, contained commands that damaged Plaintiff's computer systems by slowing Plaintiff's computer systems, using up memory on Plaintiff's computer, and frustrating Plaintiff's ability to use its computers to operate its business. Plaintiff was forced to keep its computers running longer (due to the slowed performance) which utilizes more electricity and decreases the useful life of a computer.

34. Furthermore, the computer software program, Malware, contained commands that altered Plaintiff's computer systems by destroying and rendering functionless Plaintiff's authentication systems.

35. Finally, Plaintiff was forced to incur costs and expenses associated with removing the Malware and guarding against future Malware attacks. Additionally, Plaintiff suffered significant reputational harm from the breach of its computers.

36. Defendant and his co-conspirators knew Plaintiff's computer systems would be altered and damaged and Plaintiff would suffer loss as a result of their computer software program, Malware.

37. The above alleged facts support a claim of Computer Tampering under 720 ILCS 5 § 16D-3:

Section 17-51 of the Illinois Criminal Code (720 ILCS 5/17-51) provides in part:

- a) A person commits computer tampering when he or she knowingly and without the authorization of a computer's owner or in excess of the authority granted to him or her:

\*\*\*

(4) Inserts or attempts to insert a program into a computer or computer program knowing or having reason to know that such program contains information or commands that will or may:

(A) damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer;

(B) alter, delete, or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer; or

(C) cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such program;

38. A private right of action exists under the Statute under 720 ILCS 5 § 16D-3(c).

**Count V**  
**Civil Conspiracy**

39. Plaintiff re-alleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

40. Defendant and his co-conspirators had an implied or express agreement to conspire to unlawfully trespass on Plaintiff's personal property and to install Malware on Plaintiff's computer for the purpose of gaining unauthorized access to Plaintiff's computer systems.

41. Defendant and his co-conspirators knew or should have known that access to Plaintiff's computer systems was restricted to individuals with valid credentials, that the information stored thereon was restricted to individuals with valid credentials, and that Plaintiff had not authorized them to access its computers or distributed the information.

42. Defendant and his co-conspirators each committed an unlawful act in furtherance of the conspiracy, namely installing Malware on Plaintiff's computers, providing one another with information about the vulnerabilities in Plaintiff's authentication systems, encouraging one another on Internet chat rooms to commit the tortious acts complained of herein, and participating in the subsequent distribution of information from Plaintiff's computers.

**PRAYER FOR RELIEF**

Wherefore, Plaintiff prays for the following relief.

- A. Judgment in favor of Plaintiff and awarding damages in the form of compensatory, punitive, loss of use, diminution in value and loss of enjoyment and use.
- B. Judgment in favor of Plaintiff holding Defendant joint and severally liable for the harm caused by the conspiracy.
- C. Injunctive relief enjoining further damage to Plaintiff's computers;
- D. An award of reasonable attorneys' fees, costs, and expenses; and
- E. Such further relief as this Court deems just and proper.

**Jury Demand**

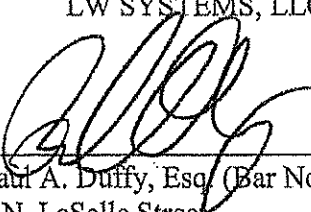
Plaintiff demands a trial by jury.

Respectfully submitted,

LW SYSTEMS, LLC

DATED: January 8, 2013

By: \_\_\_\_\_

  
Paul A. Duffy, Esq. (Bar No. 6210496)  
2 N. LaSalle Street  
13th Floor  
Chicago, IL 60602  
(312) 952-6136  
*Attorney for Plaintiff*

By: KEITH  
Kevin T. Hoerner, Esq. (Bar No. 6196686)  
Becker, Paulson, Hoerner & Thompson, P.C.  
511 West Main Street  
Belleville, IL 6226  
(618) 235-0020  
*Attorney for Plaintiff*

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

LW SYSTEMS, LLC,

Plaintiff,

v.

CHRISTOPHER HUBBARD,

Defendant.

Case No. 13-L- 15

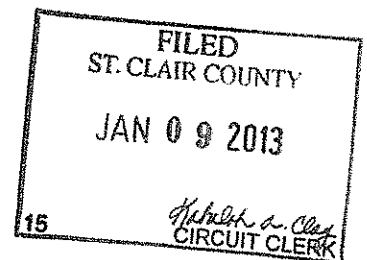
**AFFIDAVIT**

This Affidavit is made pursuant to Supreme Court Rule 222(b). Under the penalties of perjury as provided by Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the money damages sought by the Plaintiffs herein does exceed Fifty Thousand (\$50,000) Dollars.

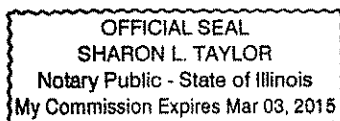
BECKER, PAULSON, HOERNER & THOMPSON, P.C.

BY:

*KTHam*  
KEVIN T. HOERNER, #6196686  
5111 West Main Street  
Belleville, Illinois 62226  
(618) 235-0020  
(618) 235-8558 Facsimile  
ATTORNEYS FOR THE PLAINTIFF



Subscribed and sworn to before me on this 9th day of January, 2013.



*Sharon L. Taylor*  
Notary Public