IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

HEALTHCARE ADVOCATES, INC., Plaintiff, v. HARDING, EARLEY, FOLLMER & FRAILEY; JOHN F.A. EARLEY, III, CHARLES L. RIDDLE, FRANK J. BONINI, JR., KIMBERLY TITUS, and JOHN DOES 1-5, Defendants.	Civil Action No. 2:05-cv-03524-RK Hon. Robert F. Kelly

PLAINTIFF HEALTHCARE ADVOCATES, INC.'S MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

McCARTER & ENGLISH, LLP
Scott S. Christie
Peter J. Boyer
Mellon Bank Center
1735 Market Street, Suite 700
Philadelphia, Pennsylvania 19103

Attorneys for Plaintiff
Healthcare Advocates, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES AND RULES

PRELIMINARY STATEMENT

Defendant Harding, Earley, Follmer & Frailey ("HEFF") is a small four-lawyer intellectual property ("IP") boutique in Valley Forge that, in addition to patent, trademark and copyright matters, practiced in the areas of Internet, e-commerce and computer law. In July 2003, HEFF represented a defendant sued by Healthcare Advocates, Inc. ("Healthcare Advocates") in an underlying federal civil lawsuit brought by Healthcare Advocates, a Philadelphia-based pioneer in the patient advocacy field.

In the course of investigating the claims in this lawsuit for its client, HEFF sought access to copyright-protected historical web page content from the Healthcare Advocates website in the digital collection of Internet Archive in California. However, Healthcare Advocates, in response to high volumes of aggressive Internet traffic directed to the Healthcare Advocates website, had followed Internet Archive's instructions and blocked public access to these archived web pages by installing a robots.txt exclusion on the computer server hosting the Healthcare Advocates website.

Rather than seek this historical web page content from the Healthcare Advocates website through the normal discovery process, representatives of HEFF unilaterally elected to access and copy as much of it as possible through the Internet Archive Wayback Machine without the authorization of either Internet Archive or Healthcare Advocates. During the period from July 9, 2003 through July 14, 2003, two HEFF attorneys and one HEFF legal assistant, supervised by the managing attorney of HEFF, discovered and exploited a vulnerability in the Wayback Machine that allowed them to bypass the robots.txt security feature and gain access to the historical web page content from the Healthcare Advocates website.

These representatives of HEFF realized that repeatedly requesting particular historical Healthcare Advocates web page content on multiple occasions within a matter of minutes would eventually cause the Wayback Machine to provide access to this web page content despite the existence of the robots.txt blocking mechanism. On July 9, 2003 and the morning of July 14, 2003, representatives of HEFF attempted to access historical web page content from the Healthcare Advocates website through the Wayback Machine on a total of 667 separate occasions. On 602 of these occasions, a representative of HEFF was presented with an access denial screen advising that the owner of the Healthcare Advocates website had blocked public access to the historical web page content for that website. In this manner, despite persistent and continuous notice that they lacked authorization, representatives of HEFF circumvented the robots.txt exclusion and managed to obtain access to historical web page content of the Healthcare Advocates website on a total of 117 separate occasions on these two days.

Representatives of HEFF were immediately aware that their conduct on July 9, 2003 and July 14, 2003 was relevant to the underlying lawsuit. Indeed, Healthcare Advocates sent representatives of HEFF several letters directing the firm to preserve the content of the hard drives from the computers used to access the historical web page content of the Healthcare Advocates website. Despite such knowledge and notice, representatives of HEFF made no effort to preserve the content of these computer hard drives until February 24, 2006, over two and one half years later. In that intervening period, data that would have been immensely valuable to Healthcare Advocates' computer forensic expert was lost.

STATEMENT OF FACTS

The facts relevant to Healthcare Advocates' Motion for Summary Judgment are set forth in detail in Plaintiff's Statement of Undisputed Material facts in Support of its Motion for

Summary Judgment ("SOF"), submitted herewith. Those facts are hereby incorporated by reference.

ARGUMENT

POINT I

SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate when there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. Fed.R.Civ.P. 56(c). An issue is genuine only if there is evidence from which a reasonable trier of fact could find in favor of the non-moving party, viewing the record as a whole in light of the evidentiary burden the law places on that party. United States v. 717 S. Woodward St., 2 F.3d 529, 533 (3d Cir. 1993). A factual dispute is material only if it might affect the outcome of the suit under the governing law. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). There are no such facts in dispute here.

While Healthcare Advocates bears the initial burden of pointing out the absence of genuine issues of material fact, the burden then shifts to the Defendants to come forward with evidence through affidavits, depositions, or admissions showing that a genuine issue exists. I.C.D. Indus. v. Fed. Ins. Co., 879 F. Supp. 480, 483 (E.D. Pa. 1995). The non-movant must make a showing sufficient to establish the existence of every element essential to his case. Anderson, 477 U.S. at 255. In other words, the party opposing the motion for summary judgment cannot rest on mere allegations and instead must present actual evidence that creates a genuine issue as to a material fact for trial. Anderson, 477 U.S. at 248; Siegel Transfer, Inc. v. Carrier Express, Inc., 54 F.3d 1125, 1130-31 (3d Cir.1995). "[U]nsupported allegations . . . and pleadings are insufficient to repel summary judgment." Schoch v. First Fid. Bancorporation, 912

F.2d 654, 657 (3d Cir.1990); see also Fed.R.Civ.P. 56(e) (requiring nonmoving party to "set forth specific facts showing that there is a genuine issue for trial").

If the non-moving party's evidence, when viewed in the context of all of the evidence, could not be credited by a rational juror, summary judgment may be granted. 717 S. Woodward St., 2 F.2d at 532. The alleged disputed facts cannot be insubstantial: A defendant can only avoid summary judgment if it establishes there is "more than...some metaphysical doubt," id. at 586, as to "facts that might affect the outcome of the suit under the governing law...." Anderson, 477 U.S. at 248. The Defendants clearly cannot meet this standard: the material facts of this case are not in dispute, and when the law is applied to the facts, judgment in favor of Healthcare Advocates is warranted on Healthcare Advocates' claims under the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act, as well as its claims for trespass and conversion.

POINT II

HEALTHCARE ADVOCATES IS ENTITLED TO SUMMARY JUDGMENT ON ITS CLAIM UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

Healthcare Advocates is entitled to summary judgment on its claim pursuant to the Digital Millennium Copyright Act (the "DMCA" or the "Act"), because Defendants' repeated unauthorized access to the copyright-protected content of the Healthcare Advocates Website[1] through the Wayback Machine on July 9, 2003 and July 14, 2003 was accomplished by circumventing the robots.txt exclusion blocking public access to this material in violation of the Act.

The DMCA states, in relevant part: "No person shall circumvent a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." 17

[1] All capitalized terms in this Memorandum of Law are defined in Plaintiff's Statement of Undisputed Material facts in Support of its Motion for Summary Judgment.

U.S.C. § 1201(a)(1)(A). The Act authorizes civil claims, providing that "any person injured by violation of 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation." 17 U.S.C. 1203(a). Section 1201(a)(1) of the DMCA governs "[t]he act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work," an act that Congress has described as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book." H.R.Rep. No. 105-551(I), 105th Cong., 2d Sess. at 17 (1998); Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, 316 (S.D.N.Y. 2000).

In order for Healthcare Advocates to prevail under this statute, it must show that a defendant (1) circumvented a technological measure that (2) effectively controls access (3) to a protected work. See DirectTV, Inc. v. Borow, 2005 WL 43261 (N.D.Ill. 2005)(granting summary judgment in favor of plaintiff on DMCA claim where defendant used devices to pirate satellite television, plaintiff used security and encryption methods to prevent non-subscribers from accessing plaintiff's signal, and plaintiff's programming content was protected by copyright). The facts are undisputed that representatives of HEFF repeatedly "broke the lock" preventing public access to copyright-protected historical web page content of the Healthcare Advocates Website, satisfying all elements of this claim.

A. Healthcare Advocates' archived website content constitutes a protected work.

Healthcare Advocates' website content is protected by copyright pursuant to 17 U.S.C. §101, *et seq*. First, on February 28, 2003 and March 26, 2003, Healthcare Advocates secured copyright registrations for its website content dating back to 1998 (U.S. Reg. Nos. TX 5-727-863, TX 5-701-306 and TX 5-786-560)(the "Copyright Registrations"), which creates a

presumption that it is the owner of valid copyrights.[2] 17 U.S.C. 410(c); Yamate USA v. Surgerman, 1991 WL 274854 at *5 (D.N.J. March 7, 1991) ("Copyright certificates produced by a plaintiff constitute *prima facie* evidence of both validity and ownership") (quotation omitted); SOF at ¶5.

Mr. Flynn did not have the assistance of legal counsel in filling out the three forms for the Copyright Registrations and, in each one, mistakenly (a) listed himself rather than Healthcare Advocates as the author; (b) signified that the website content was not a work made for hire when, in fact, it was a work made for hire; and (c) transferred ownership of the rights of copyright from himself to Healthcare Advocates. SOF at ¶6. Since the initial creation of the text and graphics comprising the Healthcare Advocates Website, Mr. Flynn had always intended that the rights of copyright in the content of the Healthcare Advocates Website be owned by Healthcare Advocates. SOF at ¶7. On November 15, 2006, Mr. Flynn submitted to the Copyright Office Forms CA to correct these mistakes in each of the Copyright Registrations, and the effective dates of supplementary registration for the Copyright Registrations is November 17, 2006 (U.S. Reg. Nos. TX-6452-052, TX-6452-053 and TX-6452-054). SOF at ¶8.

Second, even if Healthcare Advocates did not own copyright registrations, its archived website content is copyrightable because it is an "original work[] of authorship fixed in a

---

[2] Even if Plaintiff were not the owner of a valid copyright registration, Plaintiff would still be the owner of rights of copyright and would be able to bring a claim under the DMCA. "A plaintiff's failure to register its copyrighted work is not a bar to a DMCA action." I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F.Supp.2d 521, 531 n.9 (S.D.N.Y. 2004); see Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094 at *3 (E.D.Pa. Nov. 25, 2003) (stating "[w]hile a copyright registration is a prerequisite under 17 U.S.C. 411(a) for an action for copyright infringement, claims under the DMCA, however, are simply not copyright infringement claims and are separate and distinct from the latter"); see also 3 M. & D. Nimmer, Nimmer on Copyright, 12A.18[B] (2003) (noting that §1201and §1202 of the DMCA "occupy a niche distinct from copyright infringement, albeit codified in the same title of the United States Code").

tangible medium of expression," pursuant to 17 U.S.C. §102 and constitutes a "literary work" as defined in the Copyright Act. See 17 U.S.C. §102 (providing for copyright protection in original works of authorship fixed in a tangible medium of expression, and listing literary works as a category of works protected); 17 U.S.C. §101 (defining "literary works" as "works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied").

Originality, as the term is used in copyright, "means only that the work was independently created by the author, as opposed to copied from other works, and that it possesses at least some minimal degree of creativity." Nesbitt v. Schultz, 2001 WL 34131675 at *5 (M.D.Pa. May 10, 2001), citing Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991). "The requisite level of creativity is extremely low; even a slight amount will suffice. The vast majority of works make the grade quite easily, as they possess some creative spark, 'no matter how crude, humble or obvious' it might be." Nesbitt, 2001 WL 34131675 at * 5, quoting Feist Publications, 499 U.S. at 345. The text and graphics comprising the Healthcare Advocates Website from its inception in or about August 1998 through July 2003 is creative and original and constitutes an original work of authorship independently created by Mr. Flynn in his capacity as an employee of Healthcare Advocates as a work made for hire. SOF at ¶4.

Furthermore, the content of the Healthcare Advocates Website was marked with a copyright notice at all times, both when it was first published on the Healthcare Advocates Website and in the versions in the digital collection of Internet Archive protected from public access by the robots.txt exclusion. SOF at ¶9. Accordingly, when the Defendants accessed Healthcare Advocates' historical web pages through the Wayback Machine on July 9, 2003 and

July 14, 2003, they viewed these copyright notices and were thereby informed that this historical web content was protected by copyright. In view of the foregoing, the various versions of the web page content of the Healthcare Advocates Website dating back to 1998 constitute protected works under 17 U.S.C. §101, *et seq*.

B. The robots.txt exclusion is a technological measure

Healthcare Advocates employed a technological measure in the form of a robots.txt exclusion to prevent public access to the historical web page content of the Healthcare Advocates Website through the Wayback Machine in July 2003.

A robots.txt exclusion is an Internet communication protocol that is used to restrict access to an Internet website by a crawler, a computer program that scours the Internet to access and copy as much web page content of websites as possible. SOF at ¶¶27-28. A robots.txt exclusion consists of a Robots.txt Text String, a text string that a website owner inserts into a file named "robots.txt" on the computer server hosting the website. SOF at ¶29.

The robots.txt exclusion communicates with crawlers, directing whether or not these crawlers have the permission of the owner of the website to access and copy the content of the website. SOF at ¶30. A Robots.txt Text String can be configured by a website owner to communicate with all web crawlers or only to particular web crawlers. SOF at ¶31. Likewise, a Robots.txt Text String can be modified by a website owner to deny a specific crawler permission to access and copy all content of a website or just a certain potion of that website content. SOF at ¶32.

Courts have found that a variety of methods used to control access to copyrighted works constitute a "technological measure" within the meaning of the DMCA, including passwords, authentication sequences, computer software and encryptions codes. See 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F.Supp.2d 1085, 1095 (N.D.Cal. 2004)(the "CSS" encryption

program, which prevents viewing of DVD movies and copying of the data encoded on the DVD, is a "technological measure"); Sony Computer Entm't Am., Inc. v. Gamemasters, 87 F.Supp.2d 976, 987 (N.D.Cal.1999)(software on PlayStation game console that prevents unauthorized games from being played by reading encrypted data from CD to determine that CD was authorized product is a "technological measure"); Pearl Investments, LLC v. Standard I/O, Inc., 257 F.Supp.2d 326, 349-50 (D.Me.2003) (plaintiff's "encrypted, password-protected virtual private network," which blocks access to data including plaintiff's copyrighted computer software, is a "technological measure"); Realnetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. Jan. 18, 2000)(likelihood of success on the merits that plaintiff's "secret handshake" authentication sequence which controls access to plaintiff's software is a "technological measure"); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001) ("[t]he DMCA . . . backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections").

Furthermore, while not determinative, it is highly probative that technology industry leader Google, Inc. ("Google") has explicitly determined the robots.txt exclusion to be a "technological measure" in the context of controlling access to copyright-protected works. Google has embarked upon a widely-publicized initiative to partner with leading academic institutions to digitize and make publicly available the contents of these universities' libraries (the "Google Books Library Project"). The agreements that Google has signed with its university partners in the Google Books Library Project specifically address Google's obligation to restrict access to digitized books that are still protected by copyright. For example, Google's August 3, 2006 agreement with the University of California mandates:

> Google shall implement commercially reasonable technological measures (e.g., through the use of the robots.txt protocol) to restrict

> automated access to any portion of the Google Digital Copy that is in-copyright.

Agreement at ¶ 4.4; see also Google Agreement with University of Michigan at ¶ 4.5.2 ("Google shall implement technological measures (e.g., through the use of the robots.txt protocol) to restrict automated access to any portion of the Google Digital Copy or the portions of the Google website on which any portion of the Google Digital Copy is available.)

While there is no case law that explicitly finds a robots.txt exclusion to be a "technological measure" under the DMCA, it is an access denial mechanism closely analogous to a password or an authentication sequence that has been identified as such in the small number of cases that have addressed this issue. Google's embrace of the robots.txt exclusion as a technological measure restricting access to copyright-protected works in its legal agreements with universities as part of the Google Books Library Project signifies that the robots.txt exclusion has *de facto* achieved such status under the DMCA. The court should formalize that which has already gained acceptance in the industry by one of its leaders: the robots.txt exclusion is a "technological measure" under the DMCA.

C. The robots.txt exclusion effectively controls access to copyright-protected website content in the custody of Internet Archive

The DMCA provides that:

> a technological measure "effectively controls access to a work" if the measure in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the
>
> authority of the copyright owner, to gain access to the work.

17 U.S.C. § 1201(a)(3)(B). "Gain access to the work" has been defined as "the ability to enter, to obtain, or to make use of." Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546 (6th Cir. 2004).

The robots.txt exclusion effectively controls access to copyright-protected website content in the custody of Internet Archive. In July 2003, the owner of a website was able to block public access to that website's historical web pages in Internet Archive's digital collection through use of a robots.txt exclusion. SOF at ¶33. Internet Archive subscribed to a policy that honored the robots.txt exclusions of websites directed to the Internet Archive Crawler. SOF at ¶34. In accordance with this policy, the Internet Archive Crawler did not access and copy and Internet Archive did not archive and make publicly available web page content from the current versions of websites that contained a robots.txt exclusion directed to the Internet Archive Crawler. SOF at ¶35. Furthermore, Internet Archive also excluded from public access, but did not delete, existing archived web page content of websites that contained a robots.txt exclusion directed to the Internet Archive Crawler. SOF at ¶36.

A website owner could reasonably assume that by properly installing a robots.txt exclusion on the computer server hosting the website in July 2003, existing archived web page content of that website would be rendered inaccessible to the public by Internet Archive. SOF at ¶38. Accordingly, in the normal course of its operation at Internet Archive, the robots.txt exclusion directed to the Internet Archive Crawler historically has blocked access to web page content, including copyright-protected content, with a very high degree of effectiveness. SOF at ¶39.

Such effectiveness generally was evident as well in the protection accorded the historical web page content of the Healthcare Advocates Website. On July 7, 2003 or July 8, 2003, Healthcare Advocates installed a robots.txt exclusion to block access to all such web page content from public availability. SOF at ¶40. For example, the blocking mechanism apparently worked as envisioned on July 10, 2003 and July 11, 2003. See SOF at ¶¶72 & 73.

· The only reason representatives of HEFF were successful in circumventing the robots.txt exclusion on July 9, 2003 and July 14, 2003 was because they exploited a vulnerability in the Wayback Machine that allowed for the override of this blocking mechanism when subjected to a brute force attack of repeated requests for archived web page content in a span of minutes. See SOF at ¶¶43, 68 & 69. Indeed, such a relentless attack may have been a factor in causing the robots.txt exclusion to malfunction. See SOF at ¶70. At that time, the robots.txt exclusion clearly was not operating in the ordinary course. See SOF at ¶¶68 & 69. Despite that fact, the robots.txt exclusion blocking access to the historical web page content of the Healthcare Advocates Website still was able to repel the onslaught of requests for such content by representatives of HEFF and serve up the Healthcare Advocates Robots.txt Exclusion Page 90% of the time. See SOF at ¶¶48, 71 & 74.

The fact that representatives of HEFF were able to circumvent Healthcare Advocates' robots.txt exclusion at all does not render it ineffective. The level of strength of the protection afforded by the technological measure is not relevant so long as the function of the technological measure is to control access to the work. See Reimerdes 111 F.Supp.2d at 318. For example, in Reimerdes, the Southern District of New York characterized as "indefensible" the defendant's argument that the encryption software used by the plaintiff did not "effectively control" access to plaintiff's DVDs because it was a "weak cipher." Id. at 317-318. The Court reasoned that the plaintiff's encryption software "effectively controls access" to the plaintiff's copyrighted DVD movies within the meaning of the DMCA "whether or not it is a strong means of protection" because one was not able to lawfully gain access to the DVDs at issue without using one of the three keys required by the encryption software. Id. at 318; see also Lexmark, 387 F.3d at 549 ("a

precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work").

The Court in Reimerdes explained that the legislative history of the DMCA confirms this view:

> "[t]he House Judiciary Committee section-by-section analysis of the House bill, which in this respect was enacted into law, makes clear that a technological measure 'effectively controls access' to a copyrighted work if its *function* is to control access; 'The bill does define the *functions* of the technological measures that are covered – that is, what it means for a technological measure to 'effectively control access to a work' . . . and to 'effectively protect a right of a copyright owner under this title' . . . The practical, common-sense approach taken by H.R.2281 is that, if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work. . . then the 'effectiveness' test is met, and the prohibitions of the statute are applicable. This test, which focuses on the function performed by the technology, provides sufficient basis for clear interpretation.'"

Id., quoting house Comm. On Judiciary, Section-by-Section Analysis of H.R.2281 as Passed by the United States House of Representatives on August 4, 1998 at 10 (Comm.Print 1998)(emphasis in original). The Court reasoned that because, in the ordinary course of its operation, when a decryption program is not employed, the encryption code "'actually works' to prevent access to the protected work, it 'effectively controls access' within the meaning of the statute." Reimerdes, 111 F.Supp.2d at 318. The Court noted that the term "effectively" does not mean that the statute protects "only successful or efficacious technological means of controlling access" and that this interpretation "would gut the statute." Id.

Given that the purpose of the robots.txt exclusion in the ordinary course of its operation in relation to Internet Archive is to block public access to historical web page content in the custody of Internet Archive, and that Healthcare Advocates' robots.txt exclusion worked at 90% efficiency under the worst of circumstances on July 9, 2003 and July 14, 2003, this access

control mechanism effectively controls access to copyrighted works, within the meaning of the DMCA.

D. Defendants repeatedly circumvented the robots.txt exclusion protecting Healthcare Advocates' historical web page content.

To circumvent a technological measure under the DMCA means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. §1201(3)(A). Some of these prohibited actions are to be construed broadly in the realm of anti-circumvention prohibition, including the terms "avoid" and "bypass." I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F.Supp.2d 521, 532 (S.D.N.Y. 2004) (noting that "[t]hese actions are far more open-ended and mundane, and do not necessarily involve some kind of tech-based execution").

On July 7, 2003, defendant Riddle and/or defendant Bonini directed defendant Titus to attempt to access through the Wayback Machine and, if successful, to print as many of the historical web pages from the Healthcare Advocates' website as possible. SOF at ¶¶52. However, by July 9, 2003, when the representatives of HEFF began their efforts to gather this material in earnest, a robots.txt exclusion directed to the Internet Archive Crawler configured to block access to all web page content was properly implemented and in effect on the Healthcare Advocates Website. SOF at ¶¶43. This robots.txt exclusion remained in effect on July 14, 2003. Id.

Early in the day on July 9, 2003, the HEFF representatives investigated the Healthcare Advocates' robots.txt exclusion, viewing various iterations and reviewing the Frequently Asked Questions section of the Internet Archive website to learn more about this access control mechanism. See SOF at ¶¶54, 55 & 61. Not to be deterred by anything so banal as

authorization, the representatives of HEFF proceeded to bang away on their office computers, attempting to access historical web page content of the Healthcare Advocates Website on 667 separate occasions over a period of not more than nine hours total on July 9, 2003 and July 14, 2003, an average of 74 requests per hour or 1.3 requests per minute. See SOF at ¶¶71 & 74.

The robots.txt exclusion was operational as evidenced by the fact that 602 of the 667 attempted accesses yielded the Healthcare Advocates Robots.txt Exclusion Page. See SOF at ¶¶47, 71 & 74. This is the same access denial page that advised, "We're sorry, access to http://www.healthcareadvocates.com has been blocked by the site owner via robots.txt." SOF at ¶¶47-48. Yet still the representatives of HEFF persevered, studiously ignoring, on average, 67 Healthcare Advocates Robots.txt Exclusion Pages per hour or more than once per minute. See SOF at ¶¶47, 71 & 74. As a reward for their grit and determination, and exploitation of a vulnerability in the Wayback Machine, the representatives of HEFF were able to access and print historical web page content of the Healthcare Advocates Website on 117 separate occasions. See SOF at ¶¶68, 69, 71 & 74. For each successful access of historical web page content of the Healthcare Advocates Website, the representatives of HEFF first endured an average of at least five Healthcare Advocates Robots.txt Exclusion Page. See SOF at ¶¶47, 68, 69, 71 & 74.

Defendant Riddle understood at the time that all these accesses to the historical web page content of the Healthcare Advocates Website through the Wayback Machine were unauthorized. See SOF at ¶¶60 & 62. Even defendant Earley was forced to concede that the lawyers and legal assistant he managed had been on notice that they were not permitted to access the historical web page content of the Healthcare Advocates Website through the Wayback Machine. See SOF at ¶75. In light of the sheer number and frequency of accesses of Healthcare Advocates Robots.txt

Exclusion Pages by representatives of HEFF on July 9, 2003 and July 14, 2003, it would strain credibility to argue to the contrary.

Universal Studios v. Corley is instructive here. In Corley, plaintiff's encryption code security device that prevented access to DVD movies without a DVD player was described as "[i]n its basic function . . . a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products." Id. at 452-53. The court in Corley affirmed the district court's grant of an injunction against defendant's use of a DVD decryption program, which enabled the viewing of movies without using a DVD player. Id. at 453. The court reasoned that the decryption program "is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products...[The decryption program] enables anyone to gain access to a DVD movie without using a DVD player." Id.

Like the encryption code security device in Corley, Healthcare Advocate' robots.txt exclusion is the equivalent of a lock on the door to historical web page content of the Healthcare Advocates Websites in the digital collection of Internet Archive. Here, however, Defendants accessed the locked door not by fashioning a skeleton key or a lock combination, but by repeatedly pounding on that door, knowing that the lock was broken and that by banging long enough the lock would give way and the door would swing open. See SOF at ¶¶68-70.

On at least 117 separate occasions, Defendants obtained access to historical web page content of the Healthcare Advocates Website through the Wayback Machine and, in the process, avoided and bypassed, and perhaps even impaired, Healthcare Advocates' robots.txt exclusion without authorization. They clearly circumvented this technological measure that effectively

controlled access to Healthcare Advocates' copyright-protected archived web pages in violation of the DMCA.

E. Healthcare Advocates is entitled to statutory damages for Defendants' violation of the DMCA.

A plaintiff may elect to recover statutory damages under the DMCA in an action to enforce §1201. 17 U.S.C. §1203(c)(3). The statute provides that "[a]t any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer or performance of service, as the court considers just." 17 U.S.C. 1203(c)(3)(A). Healthcare Advocates is deserving of statutory damages in the amount of $2,500 per act of circumvention, times at least 117 acts of circumvention, totaling $292,500, for Defendants' willful and egregious conduct.

In determining what award of damages is "just," courts have considered the precedents concerning statutory damages under section 504(c) of the Copyright Act, such as "'the expense saved by the defendant in avoiding a licensing agreement; profits reaped by defendant in connection with the infringement; revenues lost to the plaintiff; and the willfulness of the infringement . . . The Court can also consider the goal of discouraging wrongful conduct.'" Sony Computer Entertainment America, Inc. v. Filipiak, 406 F.Supp.2d 1068, 1074-75 (N.D.Cal. 2005), quoting Controversy Music v. Shiferaw, 2003 WL 22048519 at *2 (N.D.Cal. July 7, 2003). "In the copyright infringement context, 'willful' means acting with knowledge that one's conduct constitutes copyright infringement." Filipiak, 406 F.Supp.2d at 1075, quoting Dolman v. Agee, 157 F.3d 708, 715 (9th Cir. 1990); see also In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003) ("[w]illful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement)").

Defendants' conduct in the present action is the epitome of willfulness as more fully set forth in Section II.D, supra, and incorporated herein by reference.

Moreover, this is a case tailor made for discouraging wrongful conduct in light of the identity of these defendants. This outrageous conduct was not committed by a gang of Eastern European hackers or a group of rogue computer system professionals; it was perpetrated by attorneys who purport to be officers of this court and a legal assistant under their direction and control. SOF at ¶¶ 10, 11 & 21. Furthermore, these are lawyers from an IP boutique that handle patent, trademark and copyright matters and related IP issues, including work in the area of Internet, e-commerce and computer law. SOF at ¶¶ 13 & 14. Indeed, defendant Bonini, the lawyer with primary responsibility for the Underlying Litigation that gave rise to the unauthorized accessing of historical web page content of the Healthcare Advocates Website, has the most experience within the HEFF firm in the areas of Internet, e-commerce and computer law. SOF at ¶¶ 14, 19 & 20. Moreover, defendant Earley, the managing attorney of the HEFF firm, serves as an officer of the Philadelphia Intellectual Property Law Association, a position of respect and responsibility in the legal community in general, and the IP bar in particular. SOF at ¶12. This is a group of defendants who would have been in a better position than just about anyone else to understand and appreciate the wrongfulness of their conduct. It is also a group of defendants whose treatment by the Court can potentially serve a great deal of general deterrence.

Given the willful and egregious nature of the Defendants' wrongful conduct and the goal of discouraging such conduct among other members of the bar and the public as a whole, the Court should award Healthcare Advocates the maximum amount of statutory damages recoverable under the DMCA.

POINT III

HEALTHCARE ADVOCATES IS ENTITLED TO SUMMARY JUDGMENT ON ITS CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT

Plaintiff Healthcare Advocates is entitled to summary judgment on its claims against Defendants pursuant to the Computer Fraud and Abuse Act (the "CFAA") because Defendants intentionally accessed Internet Archive's computer servers through the Wayback Machine and, in the process, obtained historical web page content of the Healthcare Advocates Website without Healthcare Advocates' authorization, causing damages to Healthcare Advocates. The CFAA provides, in relevant part, as follows:

> Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication [has violated the Act].

18 U.S.C. § 1030(a)(2)(C). The CFAA affords a civil action for any violation of the statute where a defendant's conduct caused "loss to 1 or more persons during any 1-year period . . .aggregating at least $5,000 in value." 18 U.S.C. 1030(5)(B)(i) and 1030(g) ("[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief"); see I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F.Supp.2d 521 (S.D.N.Y. 2004) (finding plaintiff had stated valid claim for civil action under 18 U.S.C. 1030(a)(2)(C) by alleging loss aggregating to at least $5,000); Theofel v. Farey-Jones, 341 F.3d 978, 986 (9th Cir. 2003)(finding civil cause of action under 1030(a)(2)(c) in conjunction with 1030(g)); In re Intuit Privacy Litig., 138 F.Supp.2d 1272, 1279 (C.D.Cal. 2001). As set forth in more detail below, Defendants clearly have caused losses to Plaintiff in excess of the $5,000 threshold. See Section III.C, infra.

A. Defendants exceeded authorized access to Internet Archive's computer servers storing its digital collection of web page content.

Defendants exceeded their authorized access of Internet Archive's computer servers in accessing historical web page content of the Healthcare Advocates Website. The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. 1030(e)(6). A computer user with authorized access to a computer and its programs, exceeds authorized access by using the programs in an unauthorized manner. See United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991)

The Senate Report on the 1996 amendments to the CFAA explains that the intent of subsection 1030(a)(2)(C) is to "protect against the interstate or foreign theft of information by computer. . . This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information." S.Rep. No. 104-357 at 3 (1996); see Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1129 (W.D. Wash. 2000) (citing Senate Report and noting that it "recognizes that someone could be liable under 1030(a)(2)(C) where intellectual property rights are involved"); Inquiry Mgmt. Sys. Ltd. v. Berkshire Info. Sys., Inc., 307 F.Supp.2d 521, 525 (S.D.N.Y. 2004) (cause of action under CFAA was adequately pled where plaintiff alleged the integrity of its copyrighted data system was impaired by defendant's copying it).

Defendants' conduct fits squarely within that prohibited by the CFAA: theft of intangible information through the use of a computer. On July 9, 2003 and July 14, 2003, the Healthcare

Advocates Website contained a viable robots.txt exclusion directed to the Internet Archive Crawler. SOF at ¶¶41 & 43. Healthcare Advocates intended that this robots.txt exclusion block public access to the historical web page content of the Healthcare Advocates Website in the digital collection of Internet Archive. SOF at ¶40. The defendants were repeatedly notified that the archived content of the Healthcare Advocates Website had been blocked by the owner of that website yet continued to attempt access and were successful in gaining access. See Section II.D, supra. Indeed, the defendants knew they were exceeding their authorized access to the Internet Archive computer servers through this conduct. Id.

Defendants' conduct was similar to that of the defendant in Southwest Airlines Co. v. Farechase, Inc., 318 F.Supp.2d 435, 439 (N.D. Tex. 2004), in which the court found that the plaintiff had sufficiently stated a cause of action under the CFAA where the defendant had accessed fare and schedule information published on plaintiff's website through the use of automatic scraping device software. The defendant argued that accessing fare and scheduling information that plaintiff published on its website was not improper as a matter of law. Id. However, the court reasoned that the plaintiff had sufficiently alleged unauthorized access, where the defendant knew that the use of such program was unauthorized because the plaintiff had directly informed the defendant that its conduct was unauthorized, and the user agreement on the plaintiff's website prohibited the use of scraper software. Id. Here, the defendants' conduct is all the more egregious since they received notice of their unauthorized access an average of at least once per minute over a span of approximately nine hours. See Section II.D, supra.

In essence, Defendants' conduct was akin to "hacking" into Internet Archive's computer servers in order to access the copyright-protected historical web page content of the Healthcare Advocates Website. See YourNetDating, LLC v. Mitchell, 88 F.Supp.2d 870 (N.D. Ill. 2000)

(finding plaintiff website owner had demonstrated a likelihood of success on its CFAA claim and granted plaintiff's request for a temporary restraining order against defendant who had "hacked" into plaintiff's website and used codes to divert users to defendant's website); Physicians Interactive v. Lathian Systems Inc., 2003 WL 23018270 at *6 (E.D.Va. December 5, 2003) (finding plaintiff was likely to succeed on the merits of its CFAA claim where defendant attacked plaintiff's website by sending "electronic robots" to steal plaintiff's customer list, computer code, and confidential data and granting preliminary injunction against defendant).

Defendants clearly exceeded their authorized access of Internet Archive's computer servers in accessing historical web page content of the Healthcare Advocates Website.

B. Through its intentional exceeding of authorized access, Defendants obtained information from a protected computer through an interstate communication.

A "protected computer" under the CFAA is defined as a computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. 1030(e)(2)(B). The computer servers housing Internet Archive's digital collection of web page content qualify as protected computers. See SOF at ¶¶ 10, 21, 22, 24 & 26. The Defendants do not dispute that they repeatedly accessed and printed historical web page content of the Healthcare Advocates Website from Internet Archive's computer servers. See SOF at ¶¶ 21, 26, 59, 64, 66, 71 & 74. Finally, all of Defendants' accesses to the computer servers housing Internet Archive's digital collection of web page content were accomplished by virtue of an interstate communication between Pennsylvania and California. See SOF at ¶¶ 10, 21 & 26.

C. Defendants' conduct caused a loss during a 1-year period aggregating at least $5,000 in value.

Defendants' conduct caused at least $5,000 in losses to Healthcare Advocates during a one-year period. The term "loss" is defined in subsection (e)(11) to include "any reasonable cost

to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, systems, or information to its condition prior to the offense." 18 U.S.C. 1030(e)(11). Such losses include remedial and investigative expenses incurred. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001). The time spent by an agent of a plaintiff to investigate and repair damage to the plaintiff's website caused by defendant's unauthorized access, such as time investigating the break-in, determining how to fix it, and taking temporary remedial measures to prevent future break-ins, has been found to be a permissible loss to be included toward the $5,000 damage threshold. See U.S. v. Middleton, 231 F.3d 1207 (9th Cir. 2000). Indeed, consequential damages resulting from the unauthorized access are cognizable under the statute. Id.

Healthcare Advocates suffered losses totaling at least in the tens of thousands of dollars, not including legal fees and costs, in direct and consequential economic harm. See SOF at ¶76. These losses have been incurred such that they total at least $5,000 in each of the years 2003 and 2006. See SOF at ¶76. Healthcare Advocates respectfully requests that upon a finding of defendants' liability under its CFAA claim, it be permitted to document and otherwise prove the full extent of its losses which will require preparing and submitting redacted legal bills to the defendants.

POINT IV

HEALTHCARE ADVOCATES' RECOVERY OF MAXIUM STATUTORY DAMAGES UNDER THE DMCA IN ADDITION TO ALL ECONOMIC DAMAGES UNDER ITS CFAA CLAIM IS WARRANTED BY DEFENDANTS' SPOLIATION OF EVIDENCE

As if Defendants' conduct as described above is not egregious enough, representatives of HEFF also have engaged in spoliation of evidence in a manner that simply shocks the conscience. As a consequence of this unbelievable conduct, critical data on the hard drives of the HEFF computers used to access historical web page content of the Healthcare Advocates

Website through the Wayback Machine that would have been immensely valuable to Healthcare Advocate's computer forensic expert is lost forever.

A party is under an obligation to preserve evidence "when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). The duty to preserve documents and information "attach[es] at the time that litigation was reasonably anticipated." Id. at 217 ("While a litigant is under no duty to keep or retain every document in its possession ... it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.") (internal citation omitted).

Each of the computers utilized by defendants Titus, Bonini and Riddle to access historical web pages of the Healthcare Advocates Website through the Wayback Machine in July 2003 contained local hard drives which stored data. SOF at ¶77. Indeed, defendant Titus may have saved historical web pages of the Healthcare Advocates Website to the local hard drive of the HEFF computer she utilized to access such web pages through the Wayback Machine in July 2003. SOF at ¶78.

In addition to data affirmatively saved by a computer user, temporary files are automatically being created and deleted on a computer's hard drive as an individual uses that computer. SOF at ¶79. Data stored on computer hard drives continually evolves and changes, even involuntarily, from day to day and even from hour to hour. SOF at ¶80. These temporary files can continue to be stored on a computer's hard drive for hours, days, weeks and even months depending upon the application responsible for creating the data. SOF at ¶81.

In July 2003, HEFF had no document retention policies, practices or protocols in place. SOF at ¶86. No representative of HEFF made any effort to determine whether, in the course of using firm computers to access historical web pages from the Healthcare Advocates Website through the Wayback Machine, data was being involuntarily sent to and saved on the hard drives of these computers. SOF at ¶87.

Nevertheless, defendant HEFF was immediately aware that the conduct of its representatives in attempting to access, accessing and printing historical web pages from the Healthcare Advocates Website through the Wayback Machine on July 9, 2003 and July 14, 2003 may be relevant to the Underlying Litigation. SOF at ¶88. As such, defendant HEFF had a duty to preserve the content of the hard drives of these computers as of July 9, 2003 and July 14, 2003. Representatives of HEFF failed to preserve the content of these hard drives on July 9, 2003 and July 14, 2003. See SOF at ¶97.

In a letter to defendant Bonini dated October 24, 2003, counsel for Healthcare Advocates and Mr. Flynn in the Underlying Litigation raised concerns that the conduct of HEFF representatives in accessing historical web pages of the Healthcare Advocates Website through the Wayback Machine in July 2003 was unauthorized and potentially in violation of Pennsylvania law. SOF at ¶89. This letter was accompanied by a subpoena requiring HEFF to designate a representative to appear and testify about this conduct and to produce relevant documents. SOF at ¶90. This letter further notified HEFF that Healthcare Advocates needed to inspect the computers used by firm representatives to access historical web pages of the Healthcare Advocates Website through the Wayback Machine. SOF at ¶91. This letter directed HEFF that "*nothing should be deleted or altered on the computers relating to the subject matter at issue and all copies of the requested documents should be preserved.*" SOF at ¶92.

In response to repeated questions about whether HEFF took any effort to preserve the contents of the hard drives of the computers used by firm representatives to access historical web pages of the Healthcare Advocates Website through the Wayback Machine in response to this October 24, 2003 letter, counsel directed defendant Earley not to answer. SOF at ¶93. Despite defendant Earley's stonewalling, Healthcare Advocates eventually learned that representatives of HEFF failed to preserve the content of these hard drives on or about October 24, 2003. See SOF at ¶97.

On May 3, 2004, counsel for Healthcare Advocates and Mr. Flynn in the Underlying Litigation filed a motion to amend their complaint to add HEFF as a defendant and to allege, *inter alia*, claims against the firm arising from the conduct of HEFF representatives using firm computers to access historical web pages of the Healthcare Advocates Website through the Wayback Machine in July 2003. SOF at ¶94. Representatives of HEFF failed to preserve the content of these hard drives on or about May 3, 2004. See SOF at ¶97.

In a letter to defendant Bonini dated July 17, 2004 and received by HEFF on July 20, 2004, Mr. Flynn stated as follows:

> Healthcare Advocates, Inc. is investigating claims against your law firm for actions which involve the use of your firm's computer system(s). Please accept this letter as a letter of preservation for the evidence that may be the subject of a lawsuit. Please preserve the electronic evidence (including hard drives) from all computers that were used to access the site www.archive.org between July 1, 2003 and July 30, 2003.

Representatives of HEFF failed to preserve the content of these hard drives on or about July 20, 2004. See SOF at ¶97.

On July 8, 2005, plaintiff Healthcare Advocates filed the Complaint in this action alleging that representatives of HEFF used firm computers to gain repeated unauthorized access to historical web pages of the Healthcare Advocates Website through the Wayback Machine on

July 9, 2003 and July 14, 2003. SOF at ¶96. Representatives of HEFF failed to preserve the content of these hard drives on or about July 8, 2005. See SOF at ¶97.

Inexplicably, the hard drives in the computers utilized by defendants Titus, Bonini and Riddle to access historical web pages of the Healthcare Advocates Website through the Wayback Machine during the period from July 9, 2003 through July 14, 2003 remained in continuous use by those computers **for over two and one half years**. See SOF at ¶97. Representatives of HEFF finally made an effort to preserve the contents of the hard drives from the firm computers on February 24, 2006, when defendant Riddle shipped these computers containing these hard drives to HEFF's computer forensic expert in Massachusetts. SOF at ¶97. By that time, any probative information on these hard drives ceased to exist. See SOF at ¶¶79-80. Consequently, we will never know the extent to which defendant Titus electronically saved copies of the historical web page content of the Healthcare Advocates Website that she accessed and printed. See SOF at ¶78.

If the data on the hard drives of the HEFF computers used to access historical web pages of the Healthcare Advocates Website through the Wayback Machine on July 9, 2003 and July 14, 2003 had been preserved immediately by representatives of HEFF, it may have been possible to determine precisely which Internet web browsers and other applications were used to facilitate such access and the identity of the HEFF representatives at the keyboards of these computers at relevant times. SOF at ¶82. In particular, the Internet browser cache from the hard drives of these HEFF computers as well as a timeline of files used during the period July 9, 2003 through July 14, 2003 would have been available, and that data would have been immensely valuable. SOF at ¶83.

Indeed, any relevant data would have been helpful to Healthcare Advocates' computer forensic expert. When attempting to analyze Internet communications and website accesses that occurred years ago, a computer forensic analyst can never have too much data to review. SOF at ¶84. Under those circumstances, the more data available to a computer forensic analyst, the better the chances that an analysis will be successful. SOF at ¶85.

Courts can impose a variety of sanctions based upon a party's spoliation of evidence, ranging from "dismissal of a claim or granting judgment in favor of a prejudiced party; suppression of evidence; an adverse inference, referred to as the spoliation inference; fines; and attorneys' fees and costs." Mosaid Technologies Inc. v. Samsung Elec. Co., Ltd., 348 F. Supp. 2d 332, 335 (D.N.J. 2004); see also Bowman v. American Medical Systems, Inc., No. Civ. A. 96-7871, 1998 WL 721079, at *3 (E.D. Pa. Oct. 9, 1998).

In Computer Associates International, Inc. v. American Fundware, Inc., plaintiff copyright owner sued defendant claiming that defendant's computer program infringed plaintiff's copyrighted computer programs. 133 F.R.D. 166, 167 (D. Colo. 1990). After commencement of the lawsuit, defendant continued to revise its allegedly infringing computer program, maintaining only the current revised version and at each revision, destroying previous versions and the underlying source code. See id. at 168. The underlying source code was critical evidence in plaintiff's copyright infringement lawsuit and plaintiff moved for a default judgment based upon defendant's destruction of such evidence during the course of pending litigation. See id.

The court, in granting plaintiff's motion for a default judgment, noted that entry of judgment against defendant was one of the "most severe sanctions available," which is "reserved for egregious offenses against an opposing party or a court." Id. at 169. The court held that

defendant was on notice of the need to preserve this evidence based not only upon service of the complaint in the action, but based upon subsequent discovery requests served upon defendant and a motion to compel production of the destroyed source code. See id. The court concluded that defendant's destruction of the source code, after being placed on notice of its importance to the issues in the case, amounted to intentional conduct that seriously prejudiced plaintiff and warranted entry of default judgment against defendant. See id. at 170.

Here, Defendants' conduct is comparable to that of the defendant in Computer Associates International. Defendant HEFF was aware as of July 9, 2003 that the conduct of its representatives in accessing historical web page content of the Healthcare Advocates Website would be relevant to the Underlying Litigation. The preservation obligation arose as of that date. Moreover, defendant HEFF was subsequently reminded on a number of occasions concerning its preservation obligation including, but certainly not limited to, October 24, 2003; May 3, 2004; July 20, 2004; and July 8, 2005. Despite repeatedly being placed on notice that these computer hard drives contained critical evidence, representatives of HEFF made no efforts to preserve their contents and, through their inaction, caused the destruction of valuable temporary files and untold other probative information and data. SOF at ¶¶ 79-83.

Healthcare Advocates recognizes that entry of judgment against Defendants based upon their destruction of evidence would be a draconian sanction. Instead, Healthcare Advocates respectfully requests that this Court, as a sanction for Defendants' spoliation of evidence, award Healthcare Advocates maximum statutory damages permissible under the DMCA in addition to all direct and consequential economic damages under its CFAA claim. This sanction is appropriate given Defendants' egregious and intentional conduct and the Court has authority to impose this lesser sanction. See Mosaid Technologies, 348 F. Supp. 2d at 335 (noting district

court's "authority to impose spoliation sanctions pursuant to the Federal Rules of Civil Procedure" and its "inherent authority.").

CONCLUSION

In view of the foregoing, all Defendants have violated the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act as a matter of law, and Healthcare Advocates is entitled to summary judgment in its favor on these claims.

Dated: February 26, 2007

By: s/ Peter J. Boyer
Scott S. Christie, Esq.
Peter J. Boyer, Esq.
McCARTER & ENGLISH, LLP
Mellon Bank Center
1735 Market Street, Suite 700
Philadelphia, Pennsylvania 19103

Attorneys for Plaintiff
Healthcare Advocates, Inc