

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION**

IN RE ASHLEY MADISON CUSTOMER )  
DATA SECURITY BREACH LITIGATION )

MDL No. 2669

**MEMORANDUM AND ORDER**

This matter is before the Court on Defendant Avid Dating Life Inc.'s Motion for Protective Order Precluding Use of Stolen Documents by Plaintiffs or their Counsel. (Doc. No. 115) The motion is fully briefed and ready for disposition.<sup>1</sup> With leave of Court, Amici Does 1 through 3 have filed an *amicus curiae* brief on the limited issue of why a protective order is required to protect the privacy interests of the class of Ashley Madison users and prevent further unlawful dissemination of the stolen documents. (Doc. No. 136) For the following reasons, the Court will grant Avid's motion in part and preclude Plaintiffs from either using or referring to the documents stolen from Avid in the computer hack of its database in the drafting of their consolidated class action complaint.

**Background**

In July 2015, a group calling itself "The Impact Team" hacked into the Ashley Madison website and threatened to expose the identities of Ashley Madison's users if its parent company, Avid, did not shut down the site. Customer records and company data were released on the internet in a series of "data dumps" after the site was not shut down pursuant to the hackers'

---

<sup>1</sup> Avid filed a notice of supplemental authority related to its motion for protective order on April 5, 2016, citing an attorney disciplinary proceeding, *In re: Joel B. Eisenstein*, No. SC 95331 (Mo. banc Apr. 5, 2016). (Doc. No. 137) In the *Eisenstein* matter, Mr. Eisenstein was suspended indefinitely for using illegally obtained evidence, including the work product of opposing counsel. Plaintiffs argue that Avid's supplemental authority provides no additional support for its motion and should be disregarded because unlike in *Eisenstein*, neither Plaintiffs nor their attorneys obtained or leaked the information at issue. (Doc. No. 139) Avid submits this supplemental authority, however, for the general principle in Missouri that ethically, an attorney may not use evidence known to be stolen or privileged.

demands. According to Avid, the hacked documents include personal information related to users of the Ashley Madison website, records of millions of credit card transactions dating to 2008, and internal company documents, including communications between Avid and its counsel. Plaintiffs assert that for purposes of drafting their consolidated amended complaint, they intend to use news articles discussing and, in some cases, quoting those documents, but not any of the original documents leaked in the data breach. (Doc. No. 130 at 2-3) Avid moves this Court to issue a protective order prohibiting Plaintiffs and their counsel from using the stolen documents for any purpose, including, but not limited to, the drafting of their consolidated class action complaint or any other future pleading, and requiring Plaintiffs and their counsel to destroy all copies of the stolen documents they possess, as well as any attorney-work product that quotes or describes the contents of the stolen documents. (Doc. No. 115 at 2)

#### **Discussion**

As a threshold matter, Plaintiffs question the Court's authority to issue a Rule 26 protective order with respect to documents obtained outside the normal discovery process, citing Kirshner v. Uniden Corp. of America, 842 F.2d 1074 (9th Cir. 1988), and Bridge C.A.T. Scan Associates v. Technicare Corp., 710 F.2d 940 (2d Cir. 1983). (Doc. No. 130 at 12-15) In Kirshner, the Ninth Circuit held it was inappropriate to require the return of purportedly privileged documents which the plaintiff's attorney had acquired in discovery in separate litigation against the same defendant. 842 F.2d at 1076. The court concluded that "a district court's power to control discovery does not extend to material discovered in a separate action, notwithstanding the fact that the parties were identical." Id. at 1081. Similarly, in Bridge, the Second Circuit found no authority for enjoining the disclosure of the defendant's trade data that had been collected by the plaintiff's attorney prior to instituting the lawsuit. 710 F.2d at 945-46.

Because the information had been “gathered independently of judicial process,” the court could not exercise control over it. Id. at 946.

Federal trial courts have, however, recognized an “inherent equitable power” to regulate the use or disclosure of information improperly obtained outside the discovery process. See, e.g., Fayemi v. Hambrecht & Quist, Inc., 174 F.R.D. 319, 326 (S.D.N.Y. 1997) (precluding party’s use of information improperly removed from his supervisor’s computer in employment discrimination action pursuant to its inherent equitable power over its own process “to prevent abuses, oppression and injustices”); Smith v. Armour Pharmaceutical Co., 838 F. Supp. 1573, 1578 (S.D. Fla. 1993) (exercising its inherent authority “to limit the use of documents obtained by means other than that court’s discovery process”); In re Shell Oil Refinery, 143 F.R.D. 105, 108-09 (E.D. La.), amended on reconsideration in part, No. CIV. A. 88-1935, 1992 WL 275426 (E.D. La. Sept. 29, 1992), and amended, 144 F.R.D. 73 (E.D. La. 1992) (limiting party’s use of documents obtained outside of the court’s discovery process “pursuant to the Court’s inherent authority to control and preserve the integrity of its judicial proceedings”); United States v. Comco Mngmt. Corp., No. SACV 08–0668, 2009 WL 4609595, at \*4-5 (C.D. Cal. Dec. 1, 2009) (ordering Government to return all of the defendants’ privileged documents it had obtained from a whistleblower pursuant to the court’s “inherent authority to grant defendants appropriate relief to remedy the Government’s circumvention of the normal discovery process”). See also Wescott Agri-Products, Inc. v. Sterling State Bank, Inc., 682 F.3d 1091, 1095 (8th Cir. 2012) (quoting Chambers v. NASCO, Inc., 501 U.S. 32, 43-46 (1991) (“By its nature as a court of justice, [a] district court possesses inherent powers ‘to manage [its] affairs so as to achieve the orderly and expeditious disposition of cases.’”).

Courts have considerable discretion in choosing an appropriate remedy under this inherent authority, Pope v. Federal Exp. Corp., 138 F.R.D. 675, 683 (W.D. Mo. 1990), aff’d in

part, vacated in part, 974 F.2d 982 (8th Cir. 1992), and may, for example, dismiss claims, compel return of all documents, restrict use of the documents at trial, disqualify counsel and award monetary sanctions. Fayemi, 174 F.R.D. at 324-27. Indeed, “a court must be able to sanction a party that seeks to introduce improperly obtained evidence; otherwise the court, by allowing the wrongdoer to utilize the information in litigation before it, becomes complicit in the misconduct.” Id. at 324.

In sum, although the Court’s authority to issue a Rule 26 protective order may be limited where evidence is obtained outside of this Court’s discovery process, the Court has the inherent equitable authority to issue an order addressing Plaintiffs’ expressed intention to use the documents at issue in this case or reports of the documents. The Court now turns to Avid’s motion.

In support of its motion, Avid argues that the use of stolen documents is improper under federal and state case law, the Rules of Professional Conduct, and ethics opinions interpreting those rules. (Doc. No. 116 at 6-9; Doc. No. 131 at 8-9) (citing 69 Am. Jur. Trials 411 § 30 (1998); American Law Institute - American Bar Association Continuing Legal Education, Corporate Internal Investigations - Legal Privileges and Ethical Issues in the Employment Law Context, SF42 ALI-ABA 927, 950 (Feb. 2001) (“Of all the ethical issues discussed in this article, this is perhaps the most clear cut. Use by counsel of stolen documents and materials, obtained either during the course of a pre-litigation investigation or during the course of a pending action, either by counsel directly or by the client and the attorney knows they are stolen, is a violation of the ethical rules.”); Ethics in Adversarial Practice, 69 Am. Jur. Trials 411 § 30 (1998) (“[m]ost jurisdictions agree that ‘tainted’ materials, in other words, those that were taken illegally or improperly obtained (as distinguished from inadvertent receipt), may not be used by a lawyer”); Iowa Practice Series, Lawyer and Judicial Ethics, § 8:4(d)(3) (“When a lawyer receives

confidential materials that he or she has reason to believe were taken from another party by a person who did not have authority to remove the documents or waive confidentiality, the lawyer may not deliberately conceal, retain, or use those stolen documents to the disadvantage of that other party”). The underlying rationale is the same whether or not the attorney wrongfully obtained the documents, that is, as officers of the court, attorneys should not possess and use property they know was stolen from the opposing party to that party’s detriment. (Doc. No. 116 at 2)

In response, Plaintiffs argue there is no basis for requiring the return of the information obtained or prohibiting its use to advance their case because the documents are not protected by any privilege, are not confidential, and because neither Plaintiffs nor their counsel were involved in any wrongdoing in obtaining the information in the first instance. (Doc. No. 130 at 10-14) Plaintiffs contend that all of the documents, including Avid’s internal business documents and documents involving communications between Avid and its counsel, have been published on the internet and in news articles reporting on the data breach and are thus in the public domain. (Id. at 2)

Plaintiffs base their entitlement to rely on this “public information” in drafting their pleadings on the fact that journalists may legally publish leaked or stolen information, and cite New York Times Co. v. United States, 403 U.S. 713 (1971), the landmark decision that made it possible for the New York Times and Washington Post to publish illegally leaked, classified documents about American involvement in the Vietnam War (the “Pentagon Papers”). (Doc. No. 130 at 2-4, 7-10; Doc. No. 139 at 2) Of course, under the First Amendment, the press is free to publish news, whatever the source. Journalists, however, are in a completely different position than parties involved in private litigation. No doubt exists that the news media enjoy the freedom

of “the press;” however, the conduct of attorneys is informed by their ethical responsibilities as officers of the Court.

Plaintiffs also cite Castano v. American Tobacco Co., 896 F. Supp. 590 (E.D. La. 1995), for the proposition that once confidential material is published on the internet, it becomes part of the public domain. (Doc. No. 130 at 4-5) In Castano, a paralegal employed by a tobacco company’s law firm allegedly took privileged documents without authorization. The company moved for a protective order to have the documents declared privileged under either the attorney-client privilege or the work product doctrine and to prohibit the plaintiffs from using the documents. The Eastern District of Louisiana denied the motion because all of the documents were in the public domain by the time of the motion. 896 F. Supp. at 595. The documents had already been disseminated to the University of California at San Francisco Medical School where they were available for copying through the university library, published on the internet, and soon to be available on CD-ROM.<sup>2</sup>

Castano is distinguishable from the instant case in that the documents at issue are not readily available to the public due in some part to the efforts of the Amici Does, on behalf of themselves and other Ashley Madison users. Amici Does assert they have gone to great effort and expense to protect their privacy interest in their consumer records by initiating legal action

---

<sup>2</sup> Some authors have questioned whether misappropriated information on the internet has truly become part of the public domain. See, e.g., Ari B. Good, Trade Secrets and the New Realities of the Internet Age, 2 Marq. Intell. Prop. L. Rev. 51 (1998); David Hricik, Confidentiality & Privilege in High-Tech Communications, 60 Tex. B.J. 104 (1997). One author argues that whether misappropriated information on the internet has become “generally known” should depend on: (1) the amount of information that was exposed; (2) the time of exposure; (3) the extent to which internet users actually accessed the information; (4) whether the disclosure was to a defined group; (5) the extent to which the information was disclosed to persons in a position to understand it; (6) whether the owner of the information took prompt action by giving notice and seeking to correct the situation by self-help and through the courts; and (7) the extent to which those who had actual access to the information relied upon or used it). Good, Trade Secrets, supra at 99-100 n. 264 (citing James Pooley, Is Nothing Secret?-The Newest Communications Medium Threatens Business Information, The Recorder, p. 4 (Nov. 6, 1996) (available in LEXIS *curnews* file)).

against the operators of websites who repurposed the stolen data to make it accessible and searchable by the media and curious internet users, which resulted in the disabling of the most prominent searchable databases. They argue that they stand to be re-victimized if the Court were to determine that the stolen documents are in the public domain. (Doc. No. 136 at 1-2) Furthermore, the documents in Castano related to issues of public concern and public health, neither of which are present in this case.

The question of whether a party may use, for any purpose, documents and information wrongfully obtained from an opposing party in prosecuting a civil action has arisen in other contexts, such as in cases where a current or former employee of a corporate defendant has surreptitiously provided documents to counsel for the plaintiff. U.S. ex rel. Rector v. Bon Secours Richmond Health Corp., No. 3:11-CV-38, 2014 WL 66714, at \*6 (E.D. Va. Jan. 6, 2014) (citing cases). In such cases, courts have precluded use of documents and information obtained outside the normal discovery process. For example, in Shell Oil, 143 F.R.D. 105, the plaintiffs' attorney surreptitiously obtained proprietary Shell documents from a disaffected Shell employee. The defendant moved for a protective order to prevent the plaintiffs from using the documents. Finding that the plaintiffs' attorney's receipt of the documents was "inappropriate and contrary to fair play," the court observed that plaintiffs "effectively circumvented the discovery process and prevented Shell from being able to argue against production." Id. at 108. The court in Shell Oil precluded the plaintiffs' use of the documents obtained from the Shell employee source or the information contained therein. Id. at 109.

Although the underlying facts in the instant case are different, particularly since there is no suggestion of impropriety on Plaintiffs' counsel's part, the outcome would be the same. Plaintiffs would be unfairly advantaged while Avid would have no opportunity to argue against production. The fact that the content of some of Avid's internal documents, including email

communications between Avid and its counsel, has been to some extent placed on the internet and reported in news articles does not change the nature of the documents. They remain stolen documents. Regardless of whether some of the documents at issue may be ultimately discoverable, Avid has, and has always had, the right to keep its own documents until met with proper discovery requests or ordered to disclose them by the Court. See Conn v. Superior Court, 196 Cal. App. 3d 774, 781 (Cal. Ct. App. 1987). The fact that Plaintiffs intend to use only news articles quoting from the original documents as opposed to the original documents themselves is, in the Court's view, a distinction without a difference. The quality and nature of the information remains the same. It is stolen information and cannot form the basis for a good faith belief of evidentiary support for a pleading.

Plaintiffs further argue that if the Court were to enter an order precluding them from using the stolen documents, then Avid would gain an unfair tactical advantage by being allowed to hide evidence of its misconduct. (Doc. No. 130 at 11 n. 6) However distasteful it may be that some of the email communications between Avid and its counsel may show wrongful or inappropriate conduct, the Court cannot and will not allow Plaintiffs to take advantage of the work of hackers to access documents outside the context of formal discovery. To do so would taint these proceedings and, if left unremedied, potentially undermine the integrity of the judicial process. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 571 (S.D.N.Y. 2008) (citing REP MCR Realty, L.L.C. v. Lynch, 363 F. Supp. 2d 984, 1012 (N.D. Ill. 2005) (“Litigants must know that the courts are not open to persons who would seek justice by fraudulent means.”) (quoting Pope, 138 F.R.D. at 683).

The internet has revolutionized the way business is conducted. As internet technology has advanced, so too has the incidence of computer-related crime such as hacking and ransomware. As noted by Amici Does, the law has struggled to keep up with the threat posed by cybercrime.



This is an evolving area of the law. Congress has enacted legislation such as the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, the Stored Communications Act, 18 U.S.C. § 2701, the Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028, as well as through updates to wiretapping laws. (Doc. No. 136 at 8) Other relevant federal statutes include the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510, and certain provisions of the USA PATRIOT Act of 2001, Public Law 107-56. Although these laws may not directly apply to the facts of this case, they illustrate the unique challenges of addressing crimes that are technology driven, and highlight the need to protect the integrity of the internet and make it a safer place for business, research and casual use. Allowing Plaintiffs to use the documents stolen from Avid would serve to encourage the conduct of hackers and cause businesses and individuals victimized by hackers to be more likely to give in to extortionists. Historically, courts have excluded evidence illegally obtained as a deterrent to the conduct, as with the exclusionary rule. While the deterrent effect in this case is indirect, it is still essential to maintain the integrity of the judicial process.

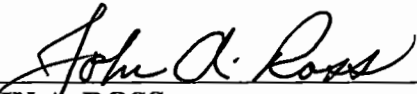
### **Conclusion**

Plaintiffs' stated intent to use the documents and information illegally obtained from Avid in the computer hack in drafting the consolidated complaint poses a threat to the integrity of this proceeding. Federal courts have the authority to remedy situations that threaten judicial integrity and the adversary process. Therefore, the Court will grant Avid's motion in part and enter an order precluding Plaintiffs and their counsel from using the documents, reports quoting the documents, and information stolen from Avid in the drafting of their consolidated class action complaint.

Accordingly,

**IT IS HEREBY ORDERED** that Defendant Avid Dating Life Inc.'s Motion for Protective Order Precluding Use of Stolen Document by Plaintiffs or their Counsel [115] is **GRANTED** in part. Plaintiffs and their counsel are hereby precluded from using or referring to the stolen documents in the consolidated class action complaint.

Dated this 29<sup>th</sup> day of April, 2016.

  
\_\_\_\_\_  
**JOHN A. ROSS**  
**UNITED STATES DISTRICT JUDGE**