United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EBATES, INC., Plaintiff, v. JOHN DOES 1-211, Defendant.	Case No. 16-cv-01925-JST **ORDER GRANTING MOTION TO PERMIT SERVICE OF SUBPOENA** Re: ECF No. 4

Before the Court is Plaintiff's Ex Parte Motion to Permit Service of Subpoena for Documents Prior to F.R.C.P. 26(f) Conference. In its motion, Plaintiff seeks to obtain early discovery to determine the identities of the unnamed defendants. The Court will grant the motion.

I. BACKGROUND

Plaintiff Ebates, Inc. identifies itself as "a pioneer and leader in the field of online cash back shopping." ECF No. 1 ("Complaint") ¶ 1. Its complaint alleges that on April 1, 2016, Ebates was the victim of a Distributed Denial of Service ("DDOS") attack by unknown parties, in which "multiple compromised systems are used to attack a specific target, causing a denial of service for users of that target." Id. ¶ 8. The attack shut down Ebates's primary website, Ebates.com, and certain other periphery properties. Id. ¶ 7.

Approximately two hours after the attack began, Ebates received a series of demands for ransom via email. Id. ¶ 10. The emails acknowledged responsibility for the attack, demanded payment via Bitcoin, and threatened that if Ebates did not pay, more attacks would follow, and Ebates would "lose customers, money, and reputation," and threatened "you will lose everything." Id. ¶ 10-11.

Ebates alleges that the ransom notes were delivered from a list of approximately 200 e-mail addresses, all of which appear to contain a first name and a random series of 4 to 5 digits.

Id. ¶ 11. It alleges that it did not pay the ransom, and was unable to restore its website for roughly 10 hours following the attack. Id. ¶ 12. It alleges it has “suffered monetary harm in the form of lost business in an amount that has not yet been determined, but likely in excess of $100,000.” Id. ¶ 13. Plaintiff brings three claims: (1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et. seq.; (2) Conversion; and (3) Trespass. Id. ¶¶ 18-27. Plaintiff also requests injunctive relief. Id. ¶ 15.

Ebates now brings this motion to serve discovery prior to a Rule 26(f) conference, requesting permission to serve subpoenas on Microsoft Corporation and Yahoo, Inc. to attempt to identify the parties behind the e-mails that sent the ransom letters.

II. LEGAL STANDARD

“As a general rule, discovery proceedings take place only after the defendant has been served; however, in rare cases, courts have made exceptions, permitting limited discovery to ensue after filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant.” Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999); see also Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980) (“In such circumstances, the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds.”).

District courts in this circuit have developed a four-part test for determining when to allow early discovery. Celestial Inc. v. Swarm Sharing Hash 8AB508AB0F9EF8B4CDB14ö248F3 C96ö5BEB882 on Dec. 15, 2011, No. CV 12-00132 DDP SSX, 2012 WL 995273, at *2 (C.D. Cal. Mar. 23, 2012). Under the test applied in Columbia Insurance Co. v. seescandy.com, the moving party must: “(1) identify the defendant with enough specificity to allow the Court to determine whether the defendant is a real person or entity who could be sued in federal court; (2) recount the steps taken to locate the defendant; (3) show that its action could survive a motion to dismiss; and (4) file a request for discovery with the Court identifying the persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information.” SBO Pictures, Inc. v. Does 1-3036, No.

United States District Court
Northern District of California

11-4220 SC, 2011 WL 6002620, at *2 (N.D. Cal. Nov. 30, 2011) (citing to Columbia Ins. Co., 185 F.R.D. at 577).

III. DISCUSSION

The Court concludes that Plaintiff has met its burden under Columbia Ins. Co. The first factor requires the Plaintiff to "identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court." Columbia Ins. Co., 185 F.R.D. at 578. "This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability can be satisfied." Id.

Here, Plaintiff has alleged there is at least one real person or entity that specifically targeted Ebates, which has its principal place of business in California, both through its DDOS attack and its ransom demands. Complaint ¶¶ 3-4. This is sufficient for the Court to conclude that the defendants are real people or entities over which the requirements of jurisdiction and justiciability "can be satisfied."

The second factor requires the Plaintiff to "identify all previous steps taken to locate the elusive defendant. Columbia Ins. Co., 185 F.R.D. at 579. "This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants." Id.

Ebates has not identified the previous steps taken to locate the unnamed defendants. However, a declaration submitted by a Senior Director at Ebates states that it is "unaware of any way the attackers can be identified using the procedures, tools, and resources available to Ebates because Ebates does not know who owns the email addresses from which the demands for ransom were sent." ECF No. 4-2 ¶ 5. Indeed, since the e-mail addresses are the only information Ebates has, it appears that obtaining further information based on that information would be the first step in attempting to identify the defendants. The Court concludes that, given these specific circumstances, Plaintiff has made "a good faith effort" to comply with service requirements and to identify the defendants.

The third factor requires Plaintiff to "establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." Columbia Ins. Co., 185 F.R.D. at 579.

While "[a] conclusory pleading will never be sufficient to satisfy this element," id., other courts in this district have held that a prima facie showing of a plausible claim is sufficient, Dallas Buyers Club LLC v. Doe-73.202.228.252, No. 16-CV-00858-PSG, 2016 WL 1138960, at *3 (N.D. Cal. Mar. 23, 2016).

The CFAA states that a person violates its provisions when, among other things, he or she:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss[.]

18 U.S.C. § 1030(a)(5).

Ebates contends that other courts have held that claims of a DDOS attack are sufficient to plead a CFAA claim, and cites to Tyco Int'l (US) Inc. v. John Does, 1-3, No. 01 CIV.3856-RCC-DF, 2003 WL 23374767, at *4 (S.D.N.Y. Aug. 29, 2003). Courts in this circuit have reached the same conclusion as well. See BHRAC, LLC v. Regency Car Rentals, LLC, No. CV 15-865-GHK MANX, 2015 WL 3561671, at *4 (C.D. Cal. June 4, 2015). At this early stage, the Court need not, and does not, resolve the question of whether Ebates has pleaded a plausible claim under the CFAA. Nevertheless, it concludes that Ebates has made the required prima facie showing.

The fourth and final factor requires the Plaintiff to "file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible." Columbia Ins. Co., 185 F.R.D. at 580. In ordering discovery to identify unnamed defendants, especially in an online context, "the need to provide injured parties with a[] forum in which they may seek redress for grievances . . . must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously." Id. at 578.

Ebates has submitted its desired subpoenas as exhibits to its motion. ECF No. 4-3. It requests that Microsoft and Yahoo provide "[a]ll [d]ocuments referring or relating to the identity of the users" of the e-mail addresses identified in its complaint, "including but not limited to documents that provide names, mailing addresses, phone numbers, billing information, date of account creation, account information and all other identifying information, including any related metadata, associated with the email addresses under any and all names, aliases, identities or designations related to the email address." Id. at 8, 16. It also requests all documents that "provide IP logs, IP address information at the tune of registration, and also between the dates March 15, 2016 and April 12, 2016, computer usage logs, or other means of recording information concerning the email or Internet usage of the email addresses," and documents of any policies or procedures that Microsoft and Yahoo have used to authenticate the identity of the persons behind the e-mail addresses. Id.

Ebates does not discuss each specific request for information, but contends that the request is "specific, targeted, and very limited," and "requests information designed to help identify the relevant individuals, such as the IP addresses and other identifying information associated with the relevant accounts." ECF No. 4 at 6. The Court concludes there is a "reasonable likelihood" that much of the information requested will lead to identifying information about the unnamed defendants. Some of the information, however, is probably unnecessary. Ebates does not explain why the phone numbers and billing information attached to the e-mail addresses are needed. See Indigital Sols., LLC v. Mohammed, No. CIV.A. H-12-2428, 2012 WL 5825824, at *3 (S.D. Tex. Nov. 15, 2012) (rejecting an early discovery request for the same information "[d]ue to the sensitive nature of this information.").

Thus, to ensure that Plaintiff's discovery does not unnecessarily reveal the private information of any parties, the Court will grant Plaintiff's request for early discovery subject to the following limitations.

1. Ebates's subpoenas may not require telephone numbers or billing information to be produced.

2. By separate order, the Court shall issue this district's model protective order for standard litigation in this case. Until further instruction by the Court, all information obtained

United States District Court
Northern District of California

from these discovery requests shall be designated confidential by Plaintiff upon its receipt. See Indigital Sols., 2012 WL 5825824, at *5.

3. Until further instruction by the Court, any filing that cites, refers to, or attaches information obtained through these discovery requests shall be filed as the subject of a motion to seal. The motion to seal shall specifically identify this order as the basis for the request to seal, and shall comply with all aspects of this Court's standing order on motions to seal.

CONCLUSION

The ex parte motion for early discovery is granted. Subject to the conditions described above, Plaintiff may serve its proposed subpoenas on Microsoft, Inc. and Yahoo, Inc.

IT IS SO ORDERED.

Dated: May 3, 2016

JON S. TIGAR
United States District Judge