

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CIVIL ACTION NO. 18-10596-GAO

NATIONAL NETWORK OF ABORTION FUNDS, EASTERN MASSACHUSETTS
ABORTION FUND, GATEWAY WOMEN'S ACCESS FUND, KENTUCKY HEALTH
JUSTICE NETWORK, NORTHWEST ABORTION ACCESS FUND, and PRETERM
ACCESS FUND,
Plaintiffs,

v.

MATTHEW JAMES DAVID¹ and JOHN DOES #1–15,
Defendants.OPINION AND ORDER

September 27, 2019

O'TOOLE, D.J.

The National Network of Abortion Funds (“NNAF”) and its co-plaintiffs are non-profit organizations that provide advocacy, outreach, and financial assistance to people seeking abortion services. They hold an annual on-line fundraiser, dubbed the National Abortion Access Bowl-a-Thon. According to their Amended Complaint, the 2016 Bowl-a-Thon “was attacked by a malicious actor or actors who hacked into the fundraising site to deliberately interrupt, block, harass, and burden the Funds’ work in providing access to abortions.” (First Am. Compl. ¶ 1 (dkt. no. 6).) “The attack shut down the Bowl-a-Thon fundraiser, costing NNAF and its member funds hundreds of thousands of dollars in lost donations, substantial fees, time, and resources to address the attack and the loss of goodwill from its donors and member organizations.” (*Id.* ¶ 2.) The complaint alleges that “Defendant Matthew James Davis (‘Davis’) is the person believed to be

¹ The caption of the plaintiffs’ amended complaint styles the name as “Matthew James David,” but the allegations identify him as “Matthew James Davis.”

primarily responsible” for the attack and disruption of the fundraising site. (Id. ¶ 11.) “Defendants John Doe Nos. 1-15 are persons who, on information and belief, may have participated in or assisted Davis in carrying out” the attack. (Id. ¶ 12.) The complaint asserts causes of action under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Freedom of Access to Clinical Entrances Act, 18 U.S.C. § 248.

Davis, who apparently resides outside this judicial district, has moved under Federal Rule of Civil Procedure 12(b)(2) to dismiss the claims as to him for want of personal jurisdiction. He has also moved for dismissal of the claims against him under Rule 12(b)(6) on the ground that the factual allegations concerning his participation in the relevant events are insufficient to state plausible claims for relief under the now-familiar Twombly-Iqbal standard. See Ashcroft v. Iqbal, 556 U.S. 662 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007).

The plaintiffs’ central factual allegations are as follows:

The 2016 fundraiser was obstructed by a person or persons who hacked into the Bowl-a-Thon website and disabled it through a distributed denial of service (“DDoS”) attack. The hacker or hackers impersonated the plaintiffs to send donors emails falsely purporting to be from the plaintiffs, and also gained access to donors’ financial and personal identifying information.

The attack began on April 7, 2016, when the hackers began searching for vulnerabilities on the plaintiffs’ online fundraising application, Blue Sky Business Application, a product of Blue Sky Collaborative.² Using JavaScript, the hackers inserted a malicious code which was later activated. On April 8, NNAF employees began noticing actions on the site which seemed suspicious, such as an anonymous account posting “strange” comments on registrant pages.³ (First

² Many of the details were learned by the plaintiffs after the attack when NNAF hired a crisis security firm to perform a post hoc forensic analysis.

³ The complaint does not say what was strange about the comments.

Am. Compl. ¶ 23.) NNAF asked Blue Sky to investigate. A few days later, on April 11, the hackers registered several accounts under names such as “qwerty,” “qwerty2,” “adolph hitler,” and “hitler.” (Id. ¶ 24.)

The next day, April 12, the website began to display the receipt of “absurdly large” donations from registered accounts, including one from the user “qwerty” for \$999,999,999. (Id. ¶ 25.) “Minutes later,” NNAF’s twitter.com account (“@abortionfunds”) received three consecutive tweets from a Twitter account called “@matthewjames.” The tweets congratulated NNAF on “passing the \$830 trillion mark” and added, “you’re gunna [sic] make little boys and girls a complete thing of the past!” (Id. ¶ 27.)

The @matthewjames Twitter account itself indicated that it belonged to “Matthew James Davis.” (Id. ¶ 28.) A website, located at www.davismj.me, connected Matthew James Davis with another website, www.Aurelia.io. That site is described as providing a “JavaScript client framework for web, mobile and desktop that leverages simple conventions to power creativity.” (Id. ¶ 28.)

That same day, the Bowl-a-Thon website appeared to receive \$66 billion in fraudulent donations through a DDoS attack which then caused the website to crash. Many of those donations were made in the name of “Adolph Hitler.” (Id. ¶ 35.) The donations were visible to all registrants for several hours. Registrants also began receiving emails alerting them to the donations.

By April 14, the hackers gained administrative access to the Blue Sky Business Application using a malicious JavaScript attack and stole personal identifying information of 2705 participants and 14,333 donors. The intruders also stole 435 credit card numbers and infected 1054 profile pages. (Id. ¶ 42–43.)

I. Personal Jurisdiction

In this case, the inquiry into whether Davis is subject to this Court’s exercise of personal jurisdiction over him collapses into the inquiry into whether the complaint plausibly alleges his involvement in the attack on the Bowl-a-Thon fundraising site. If he did what the plaintiffs suspect he did, then both the statutory and constitutional bases for personal jurisdiction would be satisfied. Contrariwise, if the complaint does not adequately allege his participation in the destructive acts as described in the complaint, then neither test would be satisfied.

II. Plausible Allegation of Liability

To survive a motion to dismiss under Rule 12(b)(6), a plaintiff must provide “enough facts to state a claim to relief that is plausible on its face.” Iqbal, 556 U.S. at 697 (quoting Twombly, 550 U.S. at 570). A complaint’s factual allegations may be “short and plain,” but they must “show[] that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). “[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not ‘show[n]’—‘that the pleader is entitled to relief.’” Iqbal, 556 U.S. at 679 (quoting Fed. R. Civ. P. 8(a)(2)). There is a difference between facts that are “consistent with” the plaintiffs’ claims and those allegations of fact that “plausibly establish” the claims. Id. at 681. The complaint’s factual allegations “must be enough to raise a right to relief above the speculative level.” Twombly, 550 U.S. at 555.

“[A]n adequate complaint must include not only a plausible claim but also a plausible defendant.” Peñalbert-Rosa v. Fortuno-Burset, 631 F.3d 592, 594 (1st Cir. 2011). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Iqbal, 556 U.S. at

678. Allegations which fail to cross the critical line “between possibility and plausibility,” Twombly, 550 U.S. at 546, are insufficient to sustain a claim.

The plaintiffs suggest three reasons why it is plausible to conclude that Davis was responsible for the attack on the fundraising site. First, they argue that he is an adept programmer who uses JavaScript, just as the hackers did. That is not much different from alleging that because he wrote his tweets in English, like the hacker comments, he is plausibly the hacker. One market report recently concluded that JavaScript is used as client-side programming language by 95.1% of all websites surveyed. W³Techns, Usage statistics of JavaScript as client-side programming language on websites, <https://w3techs.com/technologies/details/cp-javascript/all/all> (last visited September 27, 2019); see also Stack Overflow, Developer Survey Results 2019, <https://insights.stackoverflow.com/survey/2019> (last visited September 27, 2019) (identifying JavaScript as the most commonly used programming language for the seventh year in a row). The fact that Davis uses JavaScript does not distinguish him from millions of other users of that language, and consequently fails even to suggest that it is plausible that he committed the hack.

Second, the plaintiffs argue that he and the hackers used similar references, such as an allusion to genocide, in their respective comments. If Davis and the hackers had used identical or substantially similar phrases or slogans, the plaintiffs would have a point. But it should not be surprising that people who share similar views would make similar comments using similar expressions. Partisans in social policy debates often use similar-sounding slogans to press their points. The plaintiffs suggest a verbal fingerprint, but the facts alleged do not support that contention.

Finally, the plaintiffs point out that Davis’s tweets occurred shortly after the attack on the public fundraising site began, suggesting that he knew the attack was coming and chimed in as

soon as it went public, much as a bomber might plant a bomb and then hurry to a vantage point to watch the explosion. That is not a crazy theory, but it is not enough to achieve the result the plaintiffs want. It is in the nature of the Twitter experience that tweets are made in response to unfolding events, and often temporally close upon those events. The inference the plaintiffs would draw from the temporal proximity of event and subsequent tweet-about-event is too speculative to be considered a demonstration of plausibility.

As the First Circuit noted in Peñalbert, “there is nothing in the complaint beyond raw speculation to suggest that” Davis participated in the hack of the Bowl-a-Thon site. 631 F.3d at 594.

For the foregoing reasons, Davis’s Motion to Dismiss (dkt. no. 25) is GRANTED and the complaint is DISMISSED as to Davis.

To date, no service has been made on the original defendants, John Does (#1–15). The plaintiffs shall file a status report within fourteen (14) days from the date of this Opinion and Order as to their identities and attempts made to serve them.

It is SO ORDERED.

/s/ George A. O’Toole, Jr.
Senior United States District Judge