United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ENIGMA SOFTWARE GROUP USA LLC, Plaintiff, v. MALWAREBYTES INC., Defendant.	Case No. 17-cv-02915-EJD **ORDER DENYING DEFENDANT'S RENEWED MOTION TO DISMISS SECOND AMENDED COMPLAINT** Re: ECF No. 179

Plaintiff Enigma Software Group USA, LLC ("Enigma" or "Plaintiff") brings this suit alleging that Defendant Malwarebytes Inc. ("Malwarebytes" or "Defendant") wrongfully categorized Plaintiff's cybersecurity and anti-malware software as "malicious," a "threat," and as a Potentially Unwanted Program ("PUP"). In the operative Second Amended Complaint (the "SAC"), Plaintiff asserts claims for (1) violations of the Lanham Act; (2) violations of New York General Business Law ("NYGBL") § 349; (3) tortious interference with contractual relations; and (4) tortious interference with business relations. *See* SAC, ECF No. 140. Now pending before the Court is Defendant's Renewed Motion to Dismiss Second Amended Complaint (the "Motion"). *See* Mot., ECF No. 179. For the reasons discussed below, the Court DENIES the Motion.

I. BACKGROUND

A. Factual Allegations[1]

1. The Parties

Enigma is a Florida limited liability company that has developed cybersecurity software to

[1] This Factual Allegations section is taken in large part from the Court's prior order on Defendant's initial motion to dismiss the SAC, *see* ECF No. 162, and included here for clarity.

combat malware, ransomware, viruses, Trojans, hackers, and other problematic computer system attacks since at least 2003. SAC ¶¶ 2, 48. Enigma's flagship anti-malware product, SpyHunter 4, was an adaptive malware detection and removal tool that provided rigorous protection against the latest malware threats. *Id.* ¶ 48. SpyHunter 4 was available on the market until mid-2018, when an Enigma affiliate introduced a new anti-malware software program, SpyHunter 5. *Id.* Enigma additionally offers a PC privacy and software optimizer program known as RegHunter 2. *Id.* ¶ 49. RegHunter 2 is intended to enhance users' personal privacy by providing certain privacy tools, such as a powerful file-shredding function that ensures secure deletion and prevents unwanted recovery of deleted files. *Id.* The program also offers a privacy scan which provides for removal of web browsing history, temporary files, and other web browsing remnants. *Id.*

As part of its software offerings, Enigma allowed users to download a free scanning version of SpyHunter 4. SAC ¶ 50. This free version detected whether a computer had malware, spyware, ransomware, Trojans, rootkits, viruses or other malicious or threatening software. *Id.* SpyHunter 4 also detected PUPs based on defined objective and industry-based criteria. *Id.* In addition to the free scanning version, Enigma also gave users the option to buy the full version of SpyHunter 4 and provided users with a "Buy Now" link to do so. *Id.* The full version of SpyHunter 4 included the scanner, tools to remove and remediate malware, and other security protection features. *Id.* Enigma also previously provided users with a free version of RegHunter 2 which, among other features, scanned for and detected privacy and optimization issues and "effected certain repairs." *Id.* ¶ 51. As with SpyHunter 4, users had the option of paying for and accessing a full version of RegHunter 2, which included additional privacy tools and registry repair functions. *Id.*

Malwarebytes is a Delaware corporation headquartered in Santa Clara, California. SAC ¶ 35. Malwarebytes is a software company that has competed with Enigma in the anti-malware and internet security market since 2008. *Id.* ¶¶ 6–7. Its flagship anti-malware offerings—collectively known as "MBAM" products—directly competed with Enigma's SpyHunter 4 product for the entirety of SpyHunter 4's market life. *Id.* Moreover, Malwarebytes promotes, markets, and sells

its MBAM products as consumer and business solutions that detect and remove malware and other potentially threatening programs on users' computers. *Id.* MBAM products detect PUPs, automatically identify and list those purported PUPs as threats, and automatically quarantine those programs, blocking their operation and rendering them inaccessible for users. *Id.*

2. Malwarebytes's Identification of Enigma's Products

From Malwarebytes's inception in 2008 until October 4, 2016, MBAM products did not identify any of Enigma's products as "malicious," "threats," "PUPs", or any other label denoting an unwanted or problematic program. SAC ¶ 10. Malwarebytes also did not quarantine or block businesses or consumers from using any of Enigma's products, including SpyHunter 4 and RegHunter 2. *Id.*

On October 5, 2016, Malwarebytes revised the criteria it used to identify PUPs. *Id.* ¶ 12. The new criteria identified SpyHunter 4 and RegHunter 2 as PUPs and threats. *Id.* As a result, if a consumer had SpyHunter 4 or RegHunter 2 on his or her computer and then downloaded or scanned that computer with MBAM products, the MBAM products would automatically quarantine the Enigma products and identify them to the consumer as threats and PUPs, denying users access to the products' protection features. *Id.* ¶ 117. Once the products were quarantined, the consumer would not be able to automatically launch or use SpyHunter 4 or RegHunter 2, even if the consumer attempted to restore those programs. SAC ¶ 121. The user would have to access the "Quarantine" window and manually click the "Restore" button. *Id.* Further, Enigma alleges that subsequent attempts by the user to re-launch the Enigma product would result in another automatic quarantine by Malwarebytes's MBAM products. *Id.* Enigma alleges that if the user restarted the computer, she would still not be able to launch the Enigma program upon reboot because Malwarebytes continued to block the operation of necessary Enigma files. *Id.* Alternatively, if a user had MBAM products on her computer and then attempted to download or install SpyHunter 4 or RegHunter 2, the MBAM products would block the installation of the programs regardless of whether the consumer tried to restore them from quarantine. *Id.* ¶ 123.

Also in October 2016, Malwarebytes acquired AdwCleaner, an anti-adware product. SAC

¶ 15. AdwCleaner "identif[ies] for removal PUPs, adware, toolbars, and other unwanted software for its users." *Id.* At the time Malwarebytes acquired AdwCleaner, the product did not identify SpyHunter 4 or RegHunter 2 as PUPs and threats. *Id.* Following Malwarebytes's acquisition of AdwCleaner, the program began identifying and detecting SpyHunter 4 and RegHunter 2 as PUPs and threats, and began pre-selecting them for removal. *Id.* ¶ 16. Like MBAM products, AdwCleaner would then quarantine and block Enigma's programs. *Id.*

In December 2016, Enigma issued a press release announcing the launch of a "Countermeasure" to Malwarebytes's responses to Enigma's programs. *See* SAC ¶¶ 165–66. The Countermeasure provided users with an option to download an alternative SpyHunter 4 installer that disabled Malwarebytes's MBAM products and allowed use of SpyHunter 4 instead. *Id.* ¶ 165. Immediately after the press release, MBAM products began blocking all *.enigmasoftware.com domains and designating them "Malicious Website[s]." *Id.* ¶ 167.

Malwarebytes's official company website includes a "Malwarebytes Forum" (the "Forum") which Malwarebytes designs and advertises as a place where users can "get advice from tech experts" and "get personalized help removing adware, malware, spyware, ransomware, trojans, viruses, and more from tech experts." SAC ¶ 138 (internal alteration omitted). Malwarebytes's company representatives, spokespersons, and agents regularly post on the Forum to market, advertise, and promote Malwarebytes's products. *Id.* Enigma alleges that an individual associated with Malwarebytes in a "Trusted Advisor" role posted under the name "Aura" on the Forum, writing that Malwarebytes was "now flagging SpyHunter products following a more aggressive stance against PUP" and that "SpyHunter fits in many of the [PUP] criterias [sic]." *Id.* ¶ 141. After another Forum user mentioned that they would be canceling their subscription to SpyHunter, Aura replied: "[m]ake sure that your subscription gets [canceled] for real when you do, since there's been a lot of report[s] in the past (and even today) of users still being charged by [Enigma] for SpyHunter[.]" *Id.* Enigma alleges that Aura's statement was an example of Malwarebytes using the Forum to deliberately make deceptive, false, and misleading statements about Enigma. *See id.* ¶¶ 138–41.

In June 2018, an Enigma affiliate called EnigmaSoft released the SpyHunter 5 program, which is an adaptive malware detection and removal software designed to target a wide range of threats and potential problems to protect users' cybersecurity. *Id.* ¶ 171. According to Enigma, two months after SpyHunter 5's introduction, MBAM products began to detect, quarantine, and block SpyHunter 5 as a PUP and a threat. SAC ¶ 172. EnigmaSoft contacted Malwarebytes, requesting an explanation for and reconsideration of the designations. *Id.* ¶ 173. Malwarebytes neither provided EnigmaSoft with a formal explanation nor changed the designations of any Enigma products. *Id.*

B. Procedural History

1. Transfer from S.D.N.Y.

Enigma initiated this action in the Southern District of New York on October 7, 2016. *See* Compl., ECF No. 1. Enigma filed a First Amended Complaint ("FAC") on December 7, 2016. *See* FAC, ECF No. 33. Malwarebytes moved to dismiss the FAC for lack of personal jurisdiction and failure to state a claim or, in the alternative, to transfer the case to the Northern District of California under 28 U.S.C. § 1404. *See* ECF No. 37. The district court granted the motion to transfer and declined to reach the motion to dismiss. *See* ECF No. 67.

2. First N.D. Cal. Motion to Dismiss and Appeal

After the case was transferred to this district, Malwarebytes renewed its motion to dismiss the FAC, arguing that Enigma failed to state a claim and, in the alternative, that Malwarebytes was immune from suit as all of Enigma's claims were barred by Section 230 of the Communications Decency Act of 1996 ("Section 230"), 47 U.S.C. § 230(c)(2). *See* ECF No. 105. The Court granted the motion, holding that Malwarebytes was immune from suit under Section 230. *See* Order Granting Deft.'s Mot. Dismiss FAC ("First MTD Order"), ECF No. 105. The Court did not reach the issue of whether Enigma failed to state a claim. *See id.* Enigma appealed, and the Ninth Circuit reversed and remanded, holding that Section 230 did not apply to "blocking and filtering decisions that [we]re driven by anticompetitive animus." *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.* ("*Enigma I*"), 946 F.3d 1040, 1050 (9th Cir. 2019).

3. Second N.D. Cal. Motion to Dismiss and Appeal

On remand, Enigma filed the SAC, asserting causes of action for (1) false advertising in violation of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B); (2) deceptive and unlawful business practices in violation of NYGBL § 349; (3) tortious interference with contractual relations; and (4) tortious interference with business relations. *See* SAC ¶¶ 213–50. Malwarebytes moved to dismiss for failure to state a claim, and the Court dismissed all four claims without leave to amend. *See* Order Granting Deft.'s Mot. Dismiss SAC ("Second MTD Order"), ECF No. 162. Regarding the Lanham Act claim, the Court reasoned that Malwarebytes's challenged designations of Enigma's products were nonactionable subjective opinions rather than verifiably false statements. *See id.* at 16–17. In evaluating Enigma's remaining three claims, the Court first determined that California law applied to the claims because New York lacked personal jurisdiction over Malwarebytes. *Id.* at 15. The Court held the NYGBL § 349 claim failed for that reason alone, and reasoned that even if New York law applied, the claim failed for the same reasons as the Lanham Act claim. *See id.* at 17–18. The Court further held that the contractual relations interference claim failed to identify "a specific contractual obligation with which Malwarebytes interfered," and that the business relations interference claim failed because Enigma did not "allege any other independently wrongful conduct" beyond the unsuccessful Lanham Act and NYGBL § 349 claims. *See id.* at 18–19.

Enigma appealed, and the Ninth Circuit affirmed in part, reversed in part, and remanded for further proceedings. *See Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.* ("*Enigma II*"), 69 F.4th 665 (9th Cir. 2023). On the Lanham Act claim, the circuit court held that Malwarebytes's designations of "malicious" and "threat" were actionable statements of fact, while the designation of "potentially unwanted program"—*i.e.*, "PUP"—was too vague to be actionable. *See id.* at 672. The court declined to assess the other elements of a Lanham Act claim in the first instance, and remanded to this Court for further proceedings. *See id.* at 671 & n.2. The Ninth Circuit additionally held that Malwarebytes is subject to personal jurisdiction in New York with respect to its sales to New York customers, and accordingly concluded that New York law applied

to Enigma's state-law claims based on those transactions. *See id.* at 675–76. The court did not decide whether New York law applies to Malwarebytes's transactions with customers outside New York. *See id.* at 676. Because these two holdings removed the Court's two bases for dismissing the NYGBL claim, the Ninth Circuit also reversed that dismissal. *See id.* The Ninth Circuit also held that the SAC sufficiently pleads a claim for tortious interference with business relations, and reversed the Court's dismissal of that claim. *Id.* at 677–78. The court affirmed the dismissal of Enigma's claim for tortious interference with contractual relations. *Id.* at 678.

4. Present Motion to Dismiss

Following the Ninth Circuit's decision, Malwarebytes renewed its motion to dismiss the SAC by filing the instant Motion. *See* Mot. Enigma filed an opposition, Malwarebytes filed a reply, and the Court heard oral argument on January 17, 2024. *See* Opp'n, ECF No. 183; Reply, ECF No. 185.

II. LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion, a plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts permitting the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). The allegations must show "more than a sheer possibility that a defendant has acted unlawfully." *Id.* Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

When determining whether a claim has been stated, a district court's review is limited to the face of the complaint and judicially noticeable information. *MGIC Indem. Corp. v. Weisman*, 803 F.2d 500, 504 (9th Cir. 1986); *N. Star Int'l v. Ariz. Corp. Comm'n*, 720 F.2d 578, 581 (9th Cir. 1983). The court must accept as true all well-pleaded factual allegations and construe them in the light most favorable to the plaintiff. *Reese v. BP Expl. (Alaska) Inc.*, 643 F.3d 681, 690 (9th

Cir. 2011). The Court need not, however, "assume the truth of legal conclusions merely because they are cast in the form of factual allegations." *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam).

III. REQUEST FOR JUDICIAL NOTICE

Malwarebytes requests that the Court take judicial notice of Exhibit 1 to the Declaration of Michael H. Todisco filed in support of the instant Motion. *See* Req. Jud. Not. ("RJN") 1, ECF No. 179-1. The exhibit at issue is a copy of a public webpage from Malwarebytes's website titled "Explained: the Malwarebytes Website Protection [M]odule" and dated August 30, 2016. *See id.* at 2; Todisco Decl., Exh. 1 (the "MWB Webpage"), ECF No. 179-3.

A district court may consider material outside the pleadings without converting a motion to dismiss into a motion for summary judgment under either (1) the doctrine of judicial notice codified in Federal Rule of Evidence 201 or (2) the judicially-created doctrine of incorporation by reference. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998, 1002 (9th Cir. 2018). Federal Rule of Evidence 201 provides that a court may judicially notice a fact "not subject to reasonable dispute," *i.e.*, a fact that is "generally known" or that "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b)(1)–(2). If a judicially noticeable document contains disputed facts, the court may notice the existence of the document, but not the disputed facts therein. *See Khoja*, 899 F.3d at 999 ("[A] court cannot take judicial notice of disputed facts contained in [judicially noticeable] public records.") (citation omitted). The incorporation by reference doctrine "treats certain documents as though they are part of the complaint itself." *Id.* at 1002. The doctrine applies "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). A court generally "may assume an incorporated document's contents are true for purposes of a motion to dismiss under Rule 12(b)(6)," but "it is improper to assume the truth of an incorporated document if such assumptions only serve to dispute facts stated in a well-pleaded complaint." *Khoja*, 899 F.3d at 1003 (internal quotations omitted).

Malwarebytes argues that courts may take judicial notice of a publication, including publicly available websites, to indicate what was in the public realm at a given time, although courts may not accept as true the publication's contents. *See* RJN 2. Malwarebytes argues that the MWB Webpage is thus judicially noticeable for the purpose of introducing the existence of the information in the public realm, and that the MWB Webpage has been incorporated by reference into the SAC because the SAC alleges that Malwarebytes's use of the term "malicious" necessarily communicated to users that the designated website was harmful. *Id.* (citing SAC ¶¶ 4, 14, 224, 230). Enigma argues that the Court should decline to take judicial notice of the MWB Webpage because (1) courts are properly skeptical of information on a party's own website; (2) the MWB Webpage is not relevant to Enigma's claims about the deceptiveness of Malwarebytes's in-app designations; and (3) the SAC's references to certain pages of Malwarebytes's website is not sufficient to establish incorporation by reference. *See* RJN Opp'n 2–5, ECF No. 184.

Malwarebytes does not request that the Court take judicial notice of the truth of the MWB Webpage's contents, and Enigma does not challenge the authenticity of the MWB Webpage. *See generally* RJN; RJN Opp'n. The Court was able to verify that the page link copied at the bottom of the MWB Webpage—https://www.malwarebytes.com/blog/news/2016/08/explained-the-malwarebytes-website-protection-module—does in fact lead to the article provided by Malwarebytes, so that the MWB Webpage is publicly accessible. Courts in this district regularly take judicial notice of the existence of publicly available webpages, and the Court will likewise take judicial notice of the existence of the MWB Webpage, though not of any disputed fact therein or of the ease or difficulty of accessing its contents. *See, e.g.*, *In re Meta Pixel Tax Filing Cases*, --- F. Supp. 3d ----, 2024 WL 1251350, at *3 (N.D. Cal. Mar. 25, 2024) (taking judicial notice of existence and contents of terms of service available on defendant's website "because the document is publicly available from a source whose accuracy cannot reasonably be questioned and its contents can be accurately determined"); *Vizcarra v. Michaels Stores, Inc.*, --- F. Supp. 3d ----, 2024 WL 64747, at *5 n.2 (N.D. Cal. Jan. 5, 2024) ("The Court takes judicial notice of the existence and contents of the webpages Michaels has submitted which show certain Michaels

private brand products for sale on Amazon.com and Walmart.com.").

IV. DISCUSSION

Malwarebytes moves to dismiss each of the three claims remaining after *Enigma II*. *See* Mot. 1. The Court turns to each in turn.

A. Lanham Act

"To state a claim for false advertising under Section 43(a) of the Lanham Act, Enigma had to allege that (1) Malwarebytes made a false statement of fact in a commercial advertisement; (2) the statement deceived or had the tendency to deceive a substantial segment of its audience; (3) the deception was material, in that it was likely to influence the purchasing decision; (4) the false statement entered interstate commerce; and (5) Enigma has been or is likely to be injured as a result of the false statement." *Enigma II*, 69 F.4th at 671 (citing *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 1139 (9th Cir. 1997)). The Ninth Circuit held in *Enigma II* that Enigma had sufficiently pleaded falsity with respect to the terms "malicious" and "threats." *See id.* at 672. Malwarebytes now argues that Enigma's Lanham Act claim[2] fails because the designations of "malicious" and "threats" are neither (1) statements made "in a commercial advertisement" nor (2) materially deceptive as a matter of law. *See* Mot. 7–17.[3]

1. Commercial Advertisement

"The Lanham Act prohibits any person from misrepresenting her or another person's goods or services in 'commercial advertising or promotion.'" *Ariix, LLC v. NutriSearch Corp.*, 985 F.3d 1107, 1114–15 (9th Cir. 2021) (quoting 15 U.S.C. § 1125(a)(1)(B)). The Ninth Circuit has adopted the below definition of commercial advertising or promotion under the Lanham Act:

> (1) commercial speech, (2) by a defendant who is in commercial competition with plaintiff, (3) for the purpose of influencing consumers to buy defendant's goods or services, and (4) that is

[2] Malwarebytes structures its Motion to jointly address the Lanham Act and NYGBL claims, *see* Mot. 7–17, and Enigma responds in kind, *see* Opp'n 7–16, but the Court will evaluate the claims separately.

[3] Malwarebytes also made these arguments on appeal, but the Ninth Circuit remanded both issues to this Court to consider in the first instance. *Enigma II*, 69 F.4th at 671 n.2.

sufficiently disseminated to the relevant purchasing public.

Id. at 1115 (citing *Coastal Abstract Serv., Inc. v. First Am. Title Inc. Co.*, 173 F.3d 725, 735 (9th Cir. 1999)).[4] Malwarebytes argues that the challenged designations are not commercial advertising because they (1) are part of Malwarebytes's actual software products, rather than mere advertising, *see* Mot. 8–10, and (2) do not promote Malwarebytes's products, as the statements are made about Enigma's products and viewed by existing Malwarebytes users, *see id.* at 8–12. Enigma counters that it adequately establishes that the designations are commercial advertising because the SAC alleges that Malwarebytes makes its statements in free products that function as advertising for paid products; that Malwarebytes's speech directly references and falsely labels specific Enigma products; and that Malwarebytes's speech is economically motivated by its desire to increase sales, profits, and market position at Enigma's expense. *See* Opp'n 2, 7–12. The Court evaluates these arguments in the context of the four elements of commercial advertising.

a. Commercial Speech

The Ninth Circuit has noted that although "[c]ommercial speech is 'usually defined as speech that does no more than propose a commercial transaction,'" *Ariix*, 985 F.3d at 1115 (quoting *United States v. United Foods, Inc.*, 533 U.S. 405, 409 (2001)), courts view this definition as a "starting point" for engaging in a "fact-driven" analysis, *id.* (citations omitted). "Where the facts present a close question, 'strong support' that the speech should be characterized as commercial speech is found where [1] the speech is an advertisement,[5] [2] the speech refers to a particular product, and [3] the speaker has an economic motivation." *Hunt v. City of Los Angeles*, 638 F.3d 703, 715 (9th Cir. 2011) (citing *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66–67 (1983)). "These so-called *Bolger* factors are important guideposts, but they are not dispositive."

[4] With respect to the second element of competition, the Supreme Court has clarified that the Lanham Act does not require *direct* competition between the parties. *See Lexmark Intern., Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 136 (2014).

[5] The difficulty of the commercial speech inquiry is perhaps evidenced by the self-referential nested definitions—*i.e.*, a commercial advertisement requires commercial speech, which is in turn indicated if the speech is an advertisement.

Ariix, 985 F.3d at 1116 (citing *Bolger*, 463 U.S. at 67 n.14; *see also Dex Media West, Inc. v. City of Seattle*, 696 F.3d 952, 958 (9th Cir. 2012)).

Malwarebytes argues that there is no close question presented here because the challenged designations were made within Malwarebytes's own products and thus at the threshold do not qualify as a commercial advertisement. *See* Mot. 8–10. However, as Enigma notes, there is no categorical rule that in-product statements are immune from Lanham Act claims. *See* Opp'n 11–12. Further, the cases cited by Malwarebytes for its proposed rule are unavailing: one decision, *Vidillion, Inc. v. Pixalate, Inc.*, No. CV 18-7270, 2019 WL 13071961, at *1 (C.D. Cal. Mar. 15, 2019), does not provide sufficient information for the Court to determine whether the present case is factually analogous, and the others—including the case on which *Vidillion* relies—involve factual analyses of the commercial advertisement question, rather than a threshold test. *See Rice v. Fox Broad. Co.*, 330 F.3d 1170, 1181 (9th Cir. 2003) (finding statement made by host of broadcast show about contents of show were not commercial advertising under *Coastal Abstract* because they were not made in promotion or marketing of show, but that nearly identical statements on jacket of videotape version of show "readily satisf[ied]" criteria for commercial advertisement); *New.Net, Inc. v. Lavasoft*, 356 F. Supp. 2d 1090, 1111 (C.D. Cal. 2004) (applying *Bolger* factors and finding that challenged speech was not commercial because it occurred after conclusion of user's transaction with defendant and because it focused not on "any particular software program . . . but primarily on the larger issue of the surreptitious downloading of computer programs").

By contrast, the allegations here state that the challenged designations were made in a marketing context for a potential transaction. *Cf. Hilton v. Hallmark Cards*, 599 F.3d 894, 905 n.7 (9th Cir. 2010) (in anti-SLAPP analysis, finding Hallmark card was not advertising itself, and that mere fact of being sold for a profit did not make the card commercial speech). The Court thus finds that Enigma's allegations present a close question of whether Malwarebytes's designations of Enigma's anti-malware programs constitute commercial speech, and accordingly turns to the three *Bolger* factors. *Cf. IMDb.com Inc. v. Becerra*, 962 F.3d 1111, 1122 (9th Cir. 2020) (finding analysis of *Bolger* factors unnecessary where speech at issue—freely available public profiles of

entertainment industry professionals in an online database including content uploaded by members of the public—did not pose a close question of commercial speech).

The Court finds the first *Bolger* factor—whether the statements are an advertisement—to fall slightly in favor of the conclusion that the challenged designations are commercial speech. Although the words at issue—"malicious" and "threat"—are not themselves advertisements, Enigma has alleged facts permitting an inference in its favor that Malwarebytes makes the speech in an advertising context. For example, Enigma alleges that the designations appear during a free trial period designed to showcase Malwarebytes's product capabilities, so that the users experience "a marketing mechanism for Malwarebytes to entice users to ultimately purchase the Malwarebytes products." SAC ¶ 66. Enigma also alleges that Malwarebytes displays the challenged speech directly alongside buttons with phrases such as "Upgrade Now." *See* SAC ¶¶ 118–19 (depicting scan results with "threats" near "Upgrade Now" button).[6] Given these allegations, the Court finds that Malwarebytes's labeling of Enigma's competing anti-malware software as a "threat" or "malicious," especially when combined with the button linking the user to a payment space, is an advertisement for purportedly superior MBAM products. *See Enigma Software Grp. USA, LLC v. Bleeping Computer LLC*, 194 F. Supp. 3d 263, 294 (S.D.N.Y. 2016) (finding blog posts promoting defendant's products as superior to Enigma's and setting forth purchase links were advertisements).

The second and third *Bolger* factors—whether the speech refers to a particular product and whether the speaker has an economic motivation—also weigh in favor of commercial speech. Enigma alleges that Malwarebytes applied the challenged designations to Enigma's SpyHunter 4 and RegHunter products within Malwarebytes's own MBAM products, including AdwCleaner.

[6] Malwarebytes argues that "courts have squarely held that Enigma's 'free trial' theory is 'without merit.'" Mot. 12 (quoting *Carafano v. Metrosplash.com, Inc.*, 207 F. Supp. 2d 1055, 1074 (C.D. Cal. 2002)). *Carafano* held that challenged speech made by *users* of the defendant's products about themselves was not made commercial merely by the fact that the defendant's business was dependent on enticing free trial members to become paying members. *See* 207 F. Supp. 2d at 1074–75 (distinguishing members' speech on defendant's website from case involving a defendant's use of photos in its catalog to promote its clothing). As the speech at issue here was uttered by Malwarebytes, rather than by its users, *Carafano* has no persuasive value here.

See, e.g., SAC ¶¶ 16–17, 114, 220. Enigma also alleges that Malwarebytes has an economic motive to designate Enigma's competing anti-malware products as "threats" and "malicious," namely, to persuade users to buy MBAM products rather than Enigma's competing anti-malware products, and thereby increase Malwarebytes's sales, profits, and market position. *See id.* ¶¶ 111, 219. Further, the cases Malwarebytes cites in response to Enigma's *Bolger* arguments are inapposite because they concern, in essence, information published in a company's database about participants in a given industry, rather than statements about competitors. *See* Reply 2–3; *IMDb.com*, 962 F.3d at 1122 (finding public profiles of entertainment professionals published by operator of free database of information about movies, television shows, and video games were not commercial speech); *New.Net*, 356 F. Supp. 2d at 1111 (finding free software intended to inform users of secretly downloaded programs comparable to "a magazine whose focus is the evaluation of consumer goods," so that flagging of plaintiff's surreptitious software related to sale of domain names was not commercial speech); *Exeltis USA Inc. v. First Databank, Inc.*, 520 F. Supp. 3d 1225, 1229 (N.D. Cal. 2021) (finding database providing insurance payors with information about pharmaceutical products was not commercial speech, and noting that database did not concern defendant's products and plaintiff had not identified direct or indirect economic benefit to defendant of challenged product classifications).

The Court accordingly finds that at the present stage of the litigation, the *Bolger* factors indicate that the challenged designations of "malicious" and "threats" are commercial speech, so that Enigma's allegations satisfy the first element of a "commercial advertisement or promotion."

b. Commercial Competition Between Parties

The second element of "commercial advertising or promotion"—commercial competition between parties—is easily met, as Enigma alleges that it directly competes with Malwarebytes in the market for anti-malware and cybersecurity software. *See* SAC ¶ 1; *see also Enigma I*, 946 F.3d at 1045 (noting, in evaluating applicability of Section 230, that the action differed from other cases "in that here the parties are competitors").

c. Purpose of Influencing Consumers in Defendant's Favor

As discussed above in the Court's analysis of the *Bolger* factors, the Court finds that Enigma has sufficiently alleged that Malwarebytes made the challenged designations in an advertising context to showcase its own MBAM products. *See supra*, at Part IV(A)(1)(a). The Court accordingly concludes that Enigma has satisfied the third element of "commercial advertising or promotion" by alleging that Malwarebytes made the speech at issue with the purpose of influencing consumers in its favor.

d. Sufficiently Disseminated to the Relevant Purchasing Public

Malwarebytes argues that the challenged designations were not sufficiently disseminated to the relevant purchasing public because only existing Malwarebytes customers saw the designations. *See* Mot. 11 n.5. Enigma responds that the SAC's allegations, which must be taken as true at this stage, demonstrate that the majority of Malwarebytes users are free users and not paying customers, and that Malwarebytes's sales model relies on its free programs to function as advertisements to induce users to upgrade to paid MBAM products. *See* Opp'n 11 (citing SAC ¶¶ 64–66, 220). Enigma further argues that the SAC alleges that Malwarebytes displays the challenged designations to all consumers who seek to simultaneously deploy both Malwarebytes and Enigma products. *See id.* at 11 n.2 (citing SAC ¶¶ 222–23).

The Court finds that the SAC's allegations permit an inference that Malwarebytes disseminated the challenged designations to the relevant purchasing public. First, Enigma alleges that Malwarebytes's free version includes features such as protection from malicious websites for 14 days—after which the only function of the free version is to clean up an already-infected computer—and that Malwarebytes uses its free trial directly as a marketing mechanism for its paid MBAM products. *See* SAC ¶¶ 65–66. Second, Enigma alleges that users who had already downloaded and installed its products and subsequently ran an MBAM scan would find Enigma's products quarantined and labeled a "threat," and that Malwarebytes users who sought to download and install Enigma products would also see the "threat" label and quarantine action. *See* SAC ¶¶ 118–23. The Court infers from these allegations that the relevant public includes consumers who

seek to use products from both Malwarebytes and Enigma, and that Malwarebytes disseminated its statements to those users. Accordingly, the challenged statements were sufficiently disseminated to the relevant purchasing public. *See Coastal Abstract*, 173 F.3d at 735 ("Where the potential purchasers in the market are relatively limited in number, even a single promotional presentation to an individual purchaser may be enough to trigger the protections of the [Lanham] Act.") (citing *Seven-Up Co. v. Coca-Cola Co.*, 86 F.3d 1379, 1386 (5th Cir. 1996)); *cf. Walker & Zanger, Inc. v. Paragon Indus., Inc.*, 549 F. Supp. 2d 1168, 1182 (N.D. Cal. 2007) (finding at summary judgment that defendant's admission of directing speech to at least one nonparty was insufficient dissemination where potential purchasers were not relatively limited in number) (citing *Coastal Abstract*, 173 F.3d at 735).

Accordingly, the Court finds that Enigma has sufficiently alleged that the challenged designations of "threat" and "malicious" are commercial advertisements.

2. Materially Deceptive

A Lanham Act claim also requires a plaintiff to plausibly allege that the challenged statement "deceived or had the tendency to deceive a substantial segment of its audience" and that "the deception was material, in that it was likely to influence the purchasing decision." *Enigma II*, 69 F.4th at 671 (citing *Southland Sod Farms*, 108 F.3d at 1139). Malwarebytes argues that the challenged designations were not materially deceptive because Malwarebytes disclosed to consumers its definitions for "threat" and "malicious," as well as the specific criteria used to reach those designations, so that a reasonable consumer would understand that the challenged designations did not identify Enigma's software as malware. *See* Mot. 14–17; *see also* MWB Webpage. Malwarebytes further argues that it disclosed both that Enigma's products are not malware, but rather PUPs, and that the "threat" designation applied to Enigma's products specifically because of the PUP classification. *See id.* at 16–17. Malwarebytes concludes that because the Ninth Circuit held that the "PUP" classification was not an actionable statement of fact under the Lanham Act, the challenged designations were not materially deceptive because they were a disclosed result of the PUP classification and specifically were not statements that

Enigma's products were malware. *See id.* Enigma counters that the SAC alleges that Enigma's users sent it hundreds of complaints after viewing Malwarebytes's statements, and the complaints reflected a belief that Enigma's products were cybersecurity threats and malware, *see* Opp'n 13 (citing SAC ¶¶ 143–64); that the PUP criteria is no longer relevant following the Ninth Circuit's decision in *Enigma II*, *see id.* at 14; and that Malwarebytes's purported disclosures are entirely disconnected from the presentation of the challenged designations to users, *see id.* at 14–16.

The Court agrees with Enigma that it has sufficiently alleged that the designations of "threat" and "malicious" were materially deceptive to a substantial segment of the relevant purchasing population. Enigma alleges that it received hundreds of complaints from users of its products who had viewed Malwarebytes's designations, and that the complaints included statements indicating that the users understood the designations to identify Enigma's products as malware. *See, e.g.*, SAC ¶ 147 ("the malware bytes' program keeps detecting malware every time I try to download your software"); *id.* ¶ 149 ("Please advise why your SpyHunter and RegHunter applications are being detected as malware."). Enigma further alleges that customers canceled orders for Enigma's software and requested refunds, *see id.* ¶ 153, and the Court can accordingly infer that the statements influenced users' purchasing decisions. *See Cisco Sys., Inc. v. Beccela's Etc., LLC*, 403 F. Supp. 3d 813, 829–30 (N.D. Cal. 2019) (finding material deception sufficiently pleaded for Lanham Act claim where party alleged that misrepresentations deterred consumers from purchasing products and that party lost sales that would have been made but for false representations). The Court also finds that any conclusion as to the efficacy of Malwarebytes's disclosures, such as in the MWB Webpage, would be premature at this stage of the proceedings and run afoul of the Court's duty to find all inferences in Enigma's favor. *Cf. Benetech, Inc. v. Omni Fin. Grp., Inc.*, 116 A.D. 3d 1190, 1192 (N.Y. App. Div. 2014) (finding, in NYGBL false advertising matter, that "documentary evidence utterly refute[d] . . . plaintiff's factual allegations" and showed contested fees were conspicuously disclosed in materials tendered by plaintiff).

Accordingly, the Court finds that Enigma has sufficiently alleged that the challenged designations of "threat" and "malicious" were materially deceptive.

3. Conclusion Re: Lanham Act Claim

For the reasons discussed above, the Court rejects the two bases on which Malwarebytes moves to dismiss Enigma's Lanham Act claim, *i.e.*, that the challenged statements were neither a commercial advertisement nor materially deceptive. *See supra*, at Parts IV(A)(1)–(2). The Court will therefore deny Malwarebytes's motion to dismiss the Lanham Act claim.

B. NYGBL § 349

NYGBL § 349 declares unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. N.Y. Gen. Bus. § 349(a). To state a claim under NYGBL § 349, "a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (quoting *Koch v. Acker, Merrall & Condit Co.*, 967 N.E.2d 675, 675 (N.Y. 2012)).

Malwarebytes argues that Enigma's NYGBL claim fails along with the Lanham Act claim because Enigma does not adequately allege that (1) the challenged designations are commercial advertisements covered by the statute and (2) the designations were materially deceptive. *See* Mot. 7–17. The Court rejects these arguments for the same reasons described above with respect to the claims under the Lanham Act. *See Avon Prods., Inc. v. S.C. Johnson & Son, Inc.*, 984 F. Supp. 768, 800 (S.D.N.Y. 1997) ("The standards for bringing a claim under § 43(a) of the Lanham Act are substantially the same as those applied to claims brought under the New York common law for unfair competition and §§ 349 and 350 of the New York General Business Law.") (citations omitted). The NYGBL-specific cases cited by Malwarebytes do not dictate a different result, as they—like those identified by the Court in its Lanham Act analysis—are broadly inapposite to the present facts as alleged by Enigma. *See, e.g.*, *N.Y. Pub. Int. Rsch. Grp., Inc. v. Ins. Info. Inst.*, 554 N.Y.S.2d 590, 591 (N.Y. App. Div. 1990) (dismissing NYGBL claim where consumer advocacy plaintiffs brought action based on statements made by insurance industry mouthpiece in editorial campaign against civil suits where defendant made no effort to sell

products—let alone products in competition with any sold by plaintiffs).

Accordingly, the Court will deny Malwarebytes's motion to dismiss the NYGBL claim.

C. Tortious Interference with Business Relations

As noted above, Enigma originally brought two common law claims for tortious interference. The Ninth Circuit held that New York law applied to both claims; affirmed the Court's dismissal of Enigma's claim for tortious interference with contractual relations; and reversed and remanded the dismissal of the claim for tortious interference with business relations. *See Enigma II*, 69 F.4th at 676–78. With respect to the latter claim, the circuit court expressly "h[e]ld that Enigma sufficiently alleged the elements of a claim for tortious interference with business relations." *Id.* at 677.

Malwarebytes nonetheless argues that this Court should dismiss Enigma's claim for tortious interference with business relations for various reasons, including that the Court should find that California law applies to the claim under New York's choice of law rules and that Enigma has not met the elements under California law, and that Enigma does not sufficiently allege New York-specific conduct to state a claim under either state's law. *See* Mot. 17–20. The Court declines Malwarebytes's invitation to make such findings in direct contradiction to the Ninth Circuit's holding in *Enigma II*, and will deny the motion to dismiss the tortious interference claim with business relations that the circuit court has held to be sufficiently pleaded.

V. CONCLUSION

For the foregoing reasons, the Court hereby ORDERS as follows:

1. Malwarebytes's motion to dismiss is DENIED, and thus Enigma's claims for (1) violation of the Lanham Act, (2) violation of NYGBL § 349, and (3) tortious interference with business relations remain at issue in this action.

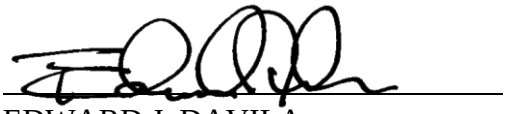
\\

\\

2. Malwarebytes shall file an answer to the three remaining claims within 14 days of the entry of this order.

IT IS SO ORDERED.

Dated: June 6, 2024



EDWARD J. DAVILA
United States District Judge