

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ASURVIO LP, a Texas limited partnership,
Plaintiff,
v.
MALWAREBYTES INC.,
Defendant.

Case No. [5:18-cv-05409-EJD](#)

**ORDER GRANTING DEFENDANT’S
MOTION TO DISMISS SECOND
AMENDED COMPLAINT**

Re: Dkt. No. 85

I. INTRODUCTION

Plaintiff Asurvio LP (“Asurvio”)¹ alleges that Malwarebytes, Inc. (“Malwarebytes”) wrongfully categorized Asurvio’s software as malware or a “Potentially Unwanted Program” (“PUP”). In its Second Amended Complaint (“SAC”), Asurvio asserts claims for (1) violation of the Lanham Act, (2) business disparagement, (3) tortious interference with contractual relations, (4) common law unfair competition and (5) violation of the Texas Theft Liability Act (“TTLA”).

Malwarebytes moves to dismiss the SAC, asserting among other things that it is entitled to immunity under section 230(c)(2)(B) of the Communications Decency Act of 1996 (“CDA”), 47 U.S.C. § 230.² The motion was heard on March 5, 2020. For the reasons set forth below, Malwarebytes’ motion will be granted.

¹ Asurvio was formerly known as PC Drivers Headquarters, LP.

² Malwarebytes’ accompanying Request for Judicial Notice of Exhibits A through C is granted. The request is unopposed and the materials are the proper subject of judicial notice. Asurvio refers to and replies upon Exhibits A and B (copies of webpages from Asurvio’s websites) in the SAC. The Court took judicial notice of Exhibit C (a webpage from Malwarebytes’ website) when ruling on Malwarebytes’ previous motion to dismiss. *See* Dkt. No. 68.

1 **II. BACKGROUND³**

2 “Asurvio provides premium full-service technical support services to consumers.” SAC ¶
 3 2. Asurvio’s services include: “(i) software solutions that work in real time in the background of
 4 the operating system to optimize processing and locate and install all missing and outdated
 5 software drivers; and (ii) technical support services for the removal of Spyware and Malware and
 6 all other facets of personal computer use.” *Id.* Asurvio uses internet search and display marketing
 7 techniques that target customers. *Id.* A potential customer may install the software from the
 8 internet and then purchase a license from Asurvio. *Id.* Asurvio pays internet search engines a fee
 9 for every consumer click that results from a consumer’s web search for Asurvio’s services. *Id.*

10 Once a customer purchases Asurvio’s software products, Asurvio’s software executes
 11 “fixes” and provides the consumer access to telephone-based human assisted technical support.
 12 *Id.* ¶ 14. Asurvio also provides “ongoing updates to new drivers as they are released by
 13 manufacturers, periodic and contextual optimizations as networking conditions change, as well as
 14 the ongoing assurance that comes from the availability of unlimited technical support regarding
 15 any issue paying customers may encounter, including the removal of Spyware/Malware.” *Id.*

16 Defendant Malwarebytes is a software company that sells malware detection software
 17 designed to scan consumer’s computers and to report to consumers in commercial advertisements
 18 or promotions any threats, PUPs, malware and viruses for de-installation. *Id.* ¶ 17. Malwarebytes
 19 gains customers by offering a free version of its software and upselling premium versions for
 20 purchase after scanning. *Id.* “Once the free version is downloaded and installed and the consumer
 21 scans his computer, Malwarebytes promotes its premium versions by allegedly identifying and
 22 quarantining alleged PUP and malware and their official websites.” *Id.*

23 In October of 2016, Malwarebytes categorized all builds and releases of Asurvio’s
 24 DRIVER SUPPORT and DRIVER DETECTIVE software with a negative PUP rating and a
 25

26 _____
 27 ³ The Background is a summary of the allegations in the SAC that are relevant to the issues raised
 in the motion to dismiss.

1 security risk to Malwarebytes' customers. *Id.* ¶ 19. Asurvio's customers who also used
 2 Malwarebytes received regular warnings from Malwarebytes that all folders of Asurvio's software
 3 were "threats" quarantined on their computers that should be uninstalled. *Id.*

4 Upon learning about the negative categorization and warnings, Asurvio contacted
 5 Malwarebytes and provided the company with information regarding Asurvio's compliance with
 6 industry leading standards and requirements, including the Clean Software Alliance ("CSA")
 7 Guidelines, Microsoft and Google's standards and other anti-malware vendor certifications by
 8 McAfee and Symantec. *Id.* ¶ 20. Malwarebytes refused to delist the negative PUP rating for
 9 Asurvio's software and referred Asurvio to AppEsteem for third party certification. *Id.* ¶¶ 20-21.
 10 AppEsteem conducted tests and issued a "clean software certification" for the current and prior
 11 builds of Asurvio's software. *Id.* ¶ 21. Asurvio informed Malwarebytes of the certification and
 12 Malwarebytes delisted Asurvio's products. *Id.*

13 In August 2017, Asurvio began listing its technical support services in its boilerplate
 14 Driver Support Service Terms and Conditions of Use and Service" (hereinafter "Terms and
 15 Conditions"). *Id.* ¶ 22 & n.1.⁴ One of the listed services under "Access to Service Via Live
 16 Technical Support Assistance" is technical support for removing Spyware/Malware. *Id.* In
 17 January 2018, Asurvio learned that Malwarebytes had relisted Asurvio's products as PUPs and
 18 was barring customers from Asurvio's websites. *Id.* By letter dated February 1, 2018, Asurvio
 19 demanded that Malwarebytes remedy the situation. *Id.* ¶ 23. Malwarebytes never formally
 20 responded to the letter. *Id.*

21 Asurvio also learned that a Malwarebytes staff member identified as "Metallica" posted
 22 "Removal instructions for Driver Support" on Malwarebytes' message board forum. *Id.* ¶ 24. The
 23 post states that Asurvio's DRIVER SUPPORT product uses "intentional false positives" and
 24 advises consumers that the best way to uninstall DRIVER SUPPORT is to use Malwarebytes'

25
 26 _____
 27 ⁴ SAC footnote 1 is a hyperlink to Asurvio's publicly available website where the Terms and
 28 Conditions are set out in full. The Court takes judicial notice of the Terms and Conditions.
 Case No.: [5:18-cv-05409-EJD](https://www.courtlistener.com/doc/5/518-cv-05409-ejd/)
 ORDER GRANTING DEFENDANT'S MOTION TO DISMISS SECOND AMENDED
 COMPLAINT

1 software. *Id.* ¶ 24. Malwarebytes is allegedly responsible for other negative comments about
2 Asurvio’s products. Malwarebytes blog “moderators” identified as “Porthos” and “exile360” have
3 described DRIVER SUPPORT as “a bogus program” and “unnecessary snake oil with no real
4 utility” that typically does more harm than good. *Id.* ¶¶ 24-25 (citing to SAC Ex. 1). In response
5 to a question about why Malwarebytes was listing DRIVER SUPPORT as a PUP, a Malwarebytes
6 blog “moderator” posted that “Driver Updates” (which is a generic term to describe Asurvio’s
7 services) are a “pure scam,” a “useless product” and “can damage your system to the point where a
8 reinstall of Windows will be needed.” *Id.* ¶ 25. Copies of these postings are attached to Asurvio’s
9 SAC.

10 Asurvio found another Internet site, www.botcrawl.com, with a post by a person named
11 Sean Doyle that contained similar comments about DRIVER SUPPORT and instructions for
12 removal. *Id.* ¶ 27. Asurvio alleges on information and belief that Sean Doyle receives monetary
13 or in-kind benefits from Malwarebytes for each sales lead or software download generated from
14 his post. *Id.* Asurvio alleges that Malwarebytes’ statements about Asurvio’s products are
15 “categorically false.” *Id.* ¶ 28.

16 Asurvio further alleges that Malwarebytes is wrongfully profiting from the use of
17 Asurvio’s products by redirecting clicks from Asurvio’s website to Malwarebytes’ website. *Id.* ¶
18 29. “When a Malwarebytes free version software user opens a search engine in his own web
19 browser and searches for DRIVER SUPPORT or ACTIVE OPTIMIZATION, Asurvio’s ads or
20 website links will prominently appear in the search engine results. However, instead of going
21 directly to Asurvio’s official website when clicking these links, it redirects consumers to the
22 Malwarebytes website for the purpose of executing a Malwarebytes sale.” *Id.* Asurvio
23 characterizes this redirection as “click misappropriation.” *Id.* ¶ 30.

24 Malwarebytes’ motion to dismiss raises three main issues: (1) whether Malwarebytes is
25 statutorily immune under CDA section 230(c)(2)(B) for providing its users with security software
26 that detects and filters Asurvio’s driver update and system optimizer software as PUPs; (2)

1 whether Malwarebytes is statutorily immune under CDA section 230(c)(1) for statements made in
2 an online forum that Malwarebytes hosts; and (3) even if Malwarebytes was not immune, whether
3 Asurvio's claims for tortious interference, common law unfair competition, and TTLA claims
4 should be dismissed for failure to state a claim.

5 **III. STANDARDS**

6 Federal Rule of Civil Procedure 8(a) requires a plaintiff to plead each claim with sufficient
7 specificity to "give the defendant fair notice of what the . . . claim is and the grounds upon which
8 it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotations omitted). The
9 factual allegations in the complaint "must be enough to raise a right to relief above the speculative
10 level" such that the claim "is plausible on its face." *Id.* at 556-57. A complaint that falls short of
11 the Rule 8(a) standard may be dismissed if it fails to state a claim upon which relief can be
12 granted. Fed. R. Civ. P. 12(b)(6). "Dismissal under Rule 12(b)(6) is appropriate only where the
13 complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory."
14 *Mendondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008).

15 When deciding whether to grant a motion to dismiss, the court must generally accept as
16 true all "well-pleaded factual allegations." *Ashcroft v. Iqbal*, 556 U.S. 662, 664 (2009). The court
17 must also construe the alleged facts in the light most favorable to the plaintiff. *See Retail Prop.*
18 *Trust v. United Bhd. of Carpenters & Joiners of Am.*, 768 F.3d 938, 945 (9th Cir. 2014) (providing
19 the court must "draw all reasonable inferences in favor of the nonmoving party" for a Rule
20 12(b)(6) motion). However, "courts are not bound to accept as true a legal conclusion couched as
21 a factual allegation." *Iqbal*, 556 U.S. at 678.

22 Also, the court usually does not consider any material beyond the pleadings for a Rule
23 12(b)(6) analysis. *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n.19
24 (9th Cir. 1989). Exceptions to this rule include material submitted as part of the complaint or
25 relied upon in the complaint, and material subject to judicial notice. *See Lee v. City of Los*
26 *Angeles*, 250 F.3d 668, 688-69 (9th Cir. 2001); *see also Branch v. Tunnell*, 14 F.3d 449, 454 (9th

27 Case No.: [5:18-cv-05409-EJD](#)

28 ORDER GRANTING DEFENDANT'S MOTION TO DISMISS SECOND AMENDED COMPLAINT

United States District Court
Northern District of California

1 Cir. 1994), *overruled on other grounds by Galbraith v. County of Santa Clara*, 307 F.3d 1119,
2 1127 (9th Cir. 2002) (“documents whose contents are alleged in a complaint and whose
3 authenticity no party questions, but which are not physically attached to the pleading, may be
4 considered in ruling on a Rule 12(b)(6) motion to dismiss”).

5 **IV. DISCUSSION**

6 **A. Section 230(c)(2)(B) Immunity**

7 The central issue presented in Malwarebytes’ motion to dismiss is whether the safe harbor
8 provision of the CDA immunizes Malwarebytes from Asurvio’s claims arising out of
9 Malwarebytes’ filtering software. The statute provides, in relevant part:

(c) Protection for “Good Samaritan” blocking and screening of
offensive material. . .

(2) Civil liability

No provider or user of an interactive computer service shall be
held liable on account of. . .

(B) any action taken to enable or make available to information
content providers or others the technical means to restrict access
to material described in paragraph (1).

16 47 U.S.C. § 230(c)(2)(B). The material that can be blocked under section 230(c)(2)(B) includes
17 “material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively
18 violent, harassing, or otherwise objectionable, whether or not such material is constitutionally
19 protected[.]” *Id.* § 230(c)(2)(A). The statute defines “interactive computer service” to mean “any
20 information service, system, or access software provider that provides or enables computer access
21 by multiple users to a computer server, including specifically a service or system that provides
22 access to the Internet and such systems operated or services offered by libraries or educational
23 institutions.” *Id.* § 230(f)(2). The statute defines “access software provider” to mean “a provider
24 of software (including client or server software), or enabling tools that do any one or more of the
25 following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest
26 content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or

1 translate content.” *Id.* § 230(f)(4)(A)-(C). “Thus, a provider of software or enabling tools that
2 filter, screen, allow, or disallow content that the provider or user considers obscene, lewd,
3 lascivious, filthy, excessively violent, harassing, or otherwise objectionable may not be held liable
4 for any action taken to make available the technical means to restrict access to that material, so
5 long as the provider enables access by multiple users to a computer server.” *Zango, Inc. v.*
6 *Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 (9th Cir. 2009). Internet users and software providers
7 have discretion to determine what online material is “otherwise objectionable.” *Id.* at 1175.
8 Congress enacted these provisions “to encourage the development of technologies which
9 maximize user control over what information is received by individuals, families, and schools who
10 use the Internet” and to “remove disincentives for the development and utilization of blocking and
11 filtering technologies.” 47 U.S.C. § 230(b)(3), (4). Section 230 immunity applies to business
12 torts. *Id.* at 1177 (citing *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1108, 1118-19 (9th Cir.
13 2007) (holding that CDA §230 immunity applies to state unfair competition and false advertising
14 actions)).

15 The breadth of the immunity available to software providers under CDA is not limitless.
16 *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1045 (9th Cir. 2019).
17 In that case, Enigma alleged that its spyware detection software was being blocked by the same
18 defendant here, Malwarebytes. Enigma brought an action against Malwarebytes, claiming that
19 Malwarebytes used its PUP-modification process “to advance a ‘bad faith campaign of unfair
20 competition’ aimed at ‘deceiving consumers and interfering with [the plaintiff’s] customer
21 relationships.’” *Id.* at 1048. This Court granted Malwarebytes’ motion to dismiss finding that
22 Malwarebytes was immune under section 230(c)(2) on all of Enigma’s claims. On appeal, the
23 Ninth Circuit reversed, holding that section 230(c)(2) “does not provide immunity for blocking a
24 competitor’s program for anticompetitive reasons.” *Id.* at 1052.

25 Here, Malwarebytes contends that section 230(c)(2)(B) immunizes it from liability for any
26 of Asurvio’s claims arising out of its filtering software because it is a user and provider of an

1 interactive computer service (“ICS”) that provides the technical means to restrict access to
2 material that Malwarebytes or its users consider objectionable. As such, Malwarebytes argues that
3 it satisfies the statutory requirements for immunity and that Asurvio cannot plead around the
4 immunity. In response, Asurvio contends that the immunity does not apply because just as in
5 *Enigma*, Malwarebytes is blocking Asurvio’s programs for anticompetitive reasons.

6 The Court finds that the limitation to section 230(c)(2)(B) immunity recognized in *Enigma*
7 does not apply to this case. In *Enigma*, the parties were “direct competitors” who sold “computer
8 security software nationwide.” *Id.* at 1047-48. Security software providers “help users identify
9 and block malicious or threatening software, termed malware, from their computers.” *Id.* at 1047.
10 Each software security provider “generates its own criteria to determine what software might
11 threaten users.” *Id.* Asurvio, by contrast, is not a computer security software provider; it does not
12 sell malware detection software designed to scan a computer and report PUPs. Rather, Asurvio
13 sells driver update software. Asurvio’s software programs “work in real time in the background of
14 the operating system to optimize processing and locate and install all missing and outdated
15 software drivers.” SAC ¶ 2. Asurvio does not allege that its DRIVER SUPPORT or ACTIVE
16 OPTIMIZATION programs provide any anti-spyware or anti-malware functionality as
17 Malwarebytes does. Instead, Asurvio alleges that among the services listed in its Terms and
18 Conditions is “technical support services for the removal of Spyware and Malware.” SAC ¶¶ 2,
19 22. Notably, this service, which appears in the fine print of the boilerplate Driver Support Terms
20 and Conditions, is apparently a secondary value added service that is only available “Via Live
21 Technical Support Assistance” and is limited to removal of Spyware and Malware (SAC ¶ & n.1);
22 Asurvio does not allege that its software programs identify and classify Spyware and Malware as a
23 primary feature. Asurvio’s technical support service is thus significantly dissimilar from computer
24 security software like Malwarebytes’ that once installed, automatically identifies and blocks
25 Spyware and Malware.

26 Asurvio next asserts that the parties are direct competitors because both offer software

1 services “to assist in the overall performance of individual computers” and both sell to “self-help”
 2 computer users. SAC ¶ 18. These users, according to Asurvio, “want their computers to run
 3 faster, whether as the result of maintaining appropriate drivers, optimizing various settings,
 4 combatting malware or viruses, applying other solutions, or likely a combination thereof.”
 5 Pl.’s Opp’n 5. Asurvio also relies on a post by a Malwarebytes message board “Expert” to show
 6 that Malwarebytes recognized Asurvio as a competitor. This “Expert” allegedly said that
 7 “Malwarebytes could provide the same technical support services offered by Asurvio.” SAC ¶ 18.
 8 If the Court were to accept Asurvio’s argument, then any developer of performance optimizing
 9 software designed for “self-help” computer users could potentially plead around the broad
 10 immunity granted by section 230(c)(2)(B) and render the statutory immunity meaningless.
 11 Asurvio does not allege, and cannot plausibly allege, that the parties are direct competitors.

12 Accordingly, all of Asurvio’s claims predicated on Malwarebytes’ filtering are subject to
 13 dismissal without leave to amend.

14 **B. Immunity Under Section 230(c)(1)**

15 Under CDA section 230(c)(1), “[n]o provider or user of an interactive computer service
 16 shall be treated as the publisher or speaker of any information provided by another information
 17 content provider.” 47 U.S.C. § 230(c)(1). An interactive computer service is “any information
 18 service, system, or access software provider that provides or enables computer access by multiple
 19 users to a computer server, including specifically a service or system that provides access to the
 20 Internet and such systems operated or services offered by libraries or educational institutions.”
 21 47 U.S.C. § 230(f)(2). “[T]he most common interactive computer services are websites.” *Fair*
 22 *Hous. Council of San Fernando Valley v. Roommates.Com*, 521 F.3d 1157, 1162 n.6 (9th Cir.
 23 2008); *see also Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1268 (9th Cir. 2016) (observing that websites
 24 are quintessential interactive computer services)).

25 Malwarebytes contends that it is immune under section 230(c)(1) for the postings on its
 26 online forum because there are no facts pleaded showing that Malwarebytes was the content

1 provider. More specifically, Malwarebytes contends that Asurvio has failed to plead facts
 2 showing that “Porthos” and “exile360” are forum “moderators,” much less any facts showing they
 3 had any express or implied authority to speak on Malwarebytes’ behalf. Asurvio counters that the
 4 forum identifies “Porthos” as a “Trusted Advisor” and “exile360” as an “Expert” (SAC Ex. 1), and
 5 that these titles and the content of their posts suggest the posts were made on Malwarebytes’
 6 behalf.

7 It is possible that Malwarebytes designated “Porthos” as a “Trusted Advisor” or “exile360”
 8 as an “Expert.” The mere possibility that Malwarebytes did so, however, is insufficient to support
 9 Asurvio’s claims. The SAC must state sufficient facts to support a plausible inference that
 10 Malwarebytes is responsible for the “Trusted Advisor” and “Expert” designations, and further that
 11 Malwarebytes is responsible for the content of the posts made by “Porthos” and “exile360.”
 12 Asurvio has failed to do so. Section 230(c)(1) immunity applies to the alleged negative statements
 13 appearing on Malwarebytes’ forum.

14 C. Additional Grounds for Dismissal

15 As discussed above, Malwarebytes is immune from suit under the CDA. Even if the
 16 immunity did not apply, all of Asurvio’s claims are subject to dismissal for failure to state a claim.
 17 Much of the Court’s rationale for dismissing these claims is captured in the Order Granting
 18 Defendant’s Motion to Dismiss (Dkt. No. 68) and will not be restated fully here. In brief, the
 19 Lanham Act and business disparagement claims fail as a matter of law because Asurvio has failed
 20 to allege sufficient facts to show that the statements at issue (*e.g.* that Asurvio’s products are
 21 PUPS, use “false positives,”⁵ are “bogus,” a “scam,” “snake oil”) are verifiably false rather than
 22 subjective opinions. Asurvio’s allegation that the statements are “categorically false” (SAC ¶ 28)
 23 is conclusory and need not be accepted as true. *ZL Techs, Inc. v. Gartner, Inc.*, 709 F. Supp. 2d
 24

25 ⁵ In its Opposition, Asurvio claims that whether its software initiates a “false positive” means
 26 whether “a driver needs to be updated when it is already updated.” Opp’n 9. Whether a driver
 27 “needs” to be updated or is “already” updated, however, is to some extent an inherently subjective
 28 evaluation. An older version of a program might be fully functional, and therefore not “need”
 updating.

United States District Court
Northern District of California

1 789, 796 (N.D. Cal. 2010) (holding that “[e]ven on a motion to dismiss, the Court need not accept
2 as true” the plaintiff’s conclusory allegations that a statement is actionable).

3 The statements discussed above are the predicate for the unfair competition claim.
4 Because the statements are not actionable, it follows that the unfair competition claim also fails as
5 a matter of law. *See Taylor Pub. Co. v. Jostens, Inc.*, 216 F.3d 465, 486 (5th Cir. 2000) (affirming
6 judgment as a matter of law on unfair competition claim because plaintiff failed to establish
7 independent substantive tort).


8 The tortious interference with contractual relations claim fails as a matter of law because
9 Asurvio fails to identify a specific contractual obligation with which Malwarebytes interfered and
10 fails to plead any facts to show Malwarebytes willfully and intentionally interfered with a specific
11 contractual obligation. *See Cuba v. Pylant*, 814 F.3d 701, 717 (5th Cir. 2016) (requiring “some
12 evidence that the defendant knowingly induced one of the contracting parties to breach its
13 obligations under a contract”). Instead, the SAC alleges that Malwarebytes identifies Asurvio’s
14 products as PUPs and instructs computer users to choose whether to continue using those
15 products.

16 **V. CONCLUSION**

17 For the reasons set forth above, Malwarebytes’ motion to dismiss is GRANTED. The
18 dismissal is without leave to amend because allowing for further amendment would be futile.

19 **IT IS SO ORDERED.**

20
21 Dated: March 26, 2020

22 
23 EDWARD J. DAVILA
24 United States District Judge