Edward P. Sangster (SNB 121041)
K&L GATES LLP
Four Embarcadero Center, Suite 1200
San Francisco, CA 94111
Telephone: 415 882 8200
Facsimile: 415 882 8220
ed.sangster@klgates.com

Terry Budd (*Admitted Pro Hac Vice*)
BUDD LAW PLLC
120 Lyndhurst Circle
Wexford, PA 15090
Telephone: 412.613.2541
terry.budd@buddlawglobal.com

Christopher M. Verdini (*Admitted Pro Hac Vice*)
Anna Shabalov (*Admitted Pro Hac Vice*)
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
Telephone: 412.355.6500
Facsimile: 412.355.6501
christopher.verdini@klgates.com
anna.shabalov@klgates.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ENIGMA SOFTWARE GROUP USA, LLC, Plaintiff, -against- MALWAREBYTES INC., Defendant.	Case No. 5:17-cv-02915-EJD **PLAINTIFF ENIGMA SOFTWARE GROUP USA, LLC'S OPPOSITION TO DEFENDANT MALWAREBYTES INC.'S MOTION TO DISMISS FIRST AMENDED COMPLAINT PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 12(b)(6)**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

ESG'S OPPOSITION TO MALWAREBYTES' MOTION TO DISMISS

Plaintiff Enigma Software Group USA, LLC ("ESG") files this Opposition to Malwarebytes Inc.'s ("Malwarebytes") Motion to Dismiss First Amended Complaint Pursuant to Federal Rule of Civil Procedure 12(b)(6) (the "Motion").

I. INTRODUCTION

There is one thing on which the parties agree—this case is about consumer choice. The root of the parties' disagreement lies in how consumer choice is protected from abusive, anticompetitive actions. Malwarebytes would have this Court believe that it is somehow promoting consumer choice by unilaterally designating its competitor's legitimate programs as "Potentially Unwanted Programs" ("PUPs") and threats, blocking those programs so that users who attempt to download and install those legitimate programs (and in some instances have even already contracted and paid for those programs), cannot do so, and creating only a confusing, labyrinthine method to bypass the block that many users simply cannot navigate. But nothing about Malwarebytes' designation of ESG's programs as PUPs has to do with helping consumers.

Rather, Malwarebytes is engaged in a pattern of unlawful, predatory and anti-competitive conduct against ESG to divert ESG's customers, harm ESG's business and gain profits for itself and to retaliate against ESG for the loss of the unfair competitive advantage it has held for years over ESG as a result of the unlawful conduct of its affiliate, Bleeping Computer LLC ("Bleeping"). Specifically, under the pretextual guise of amending its so-called PUP criteria, Malwarebytes is identifying ESG's anti-malware program SpyHunter and registry cleaner program RegHunter as PUPs and "threats" and automatically "quarantining" (*i.e.*, blocking) use of those programs by consumers who already have them installed or who are attempting to install them on their computers. To be clear, Malwarebytes does not simply provide to consumers a cautionary list or review of programs Malwarebytes looks upon unfavorably, as Consumer Reports might do. Rather, Malwarebytes programmers take purposeful action to electronically disable, *i.e.* render useless, ESG's programs (which in many cases a consumer has already purchased and paid for), including SpyHunter 4, an anti-malware program. Malwarebytes is, in effect, disrupting and disabling a

consumers' chosen computer security protection system.

Malwarebytes now asks this Court to condone its unlawful conduct by turning the so-called "Good Samaritan" provision of the Communications Decency Act ("CDA") on its head. As the Honorable Raymond C. Fisher of the Ninth Circuit incisively foresaw years ago, Malwarebytes is the antithesis of the "Good Samaritan" that the CDA is intended to protect:

> [A] blocking software provider might abuse [CDA] immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material "otherwise objectionable." Focusing for the moment on anticompetitive blocking, I am concerned that blocking software providers who flout users' choices by blocking competitors' content could hide behind § 230(c)(2)(B) when the competitor seeks to recover damages. ***I doubt Congress intended § 230(c)(2)(B) to be so forgiving.***

Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178 (9th Cir. 2009) (Fisher, J., concurring) (emphasis added). Malwarebytes is not motivated by any legitimate concern for its users' safety or protecting them from unwanted programs or malware, but rather is engaged in an anti-competitive strategy directly targeting a major competitor. ESG customers who also use Malwarebytes' software have attempted to override Malwarebytes' efforts to block ESG's programs only to be met with Malwarebytes "flout[ing]" those users' choices and denying them the use of anti-malware protection they have already purchased from ESG or are trying to download and/or purchase. Indeed, at the time it filed the First Amended Complaint ("FAC"), ESG had received more than 300 complaints from customers who cancelled their ESG accounts, requested non-renewal of their ESG subscriptions, and/or requested refunds because they found it either impossible, or too difficult, to override Malwarebytes' block of ESG's programs. These facts, along with the many other particularized allegations in the FAC detailing Malwarebytes' ongoing predatory conduct, not only defeat Malwarebytes' CDA defense but also demonstrate that ESG's claims of false advertising, unfair competition and tortious interference are much more than plausible and cannot be dismissed under Rule 12(b)(6).

At bottom, Malwarebytes must answer for its unlawful anti-competitive efforts that harm ESG and that ultimately strip consumers, by forcibly blocking software, of their individual right to decide what anti-malware protection best guards them in the high-risk context of computer hacking

and theft of personal identities and confidential business information.

II. ISSUES TO BE DECIDED

1. Whether Malwarebytes has no immunity under CDA § 230(c)(2) because it has unilaterally and in bad faith deemed ESG's programs PUPs despite knowing they are legitimate?

2. Whether ESG has properly pled its claims under Section 43(a) of the Lanham Act and New York General Business Law Section 349 because it has alleged false and misleading statements made in commercial advertising or promotion?

3. Whether ESG has properly pled its tortious interference claims where it identified relations with which Malwarebytes interfered and alleged breach or disruption and Malwarebytes' knowledge and intent?

III. ALLEGATIONS AND PROCEDURAL BACKGROUND

ESG is an established computer security company whose consumer security protection anti-malware flagship product SpyHunter has protected millions from malware, system breaches, and identity theft. *See* FAC, Dkt. 33, ¶¶ 1, 45. SpyHunter and ESG's advanced Windows registry cleaner, RegHunter, have received top industry certifications. ¶¶ 46-47, 52. Malwarebytes competes with ESG in the anti-malware and Internet security market.[1] ¶¶ 3-4, 54. Its flagship product, MBAM, competes directly with SpyHunter. ¶¶ 4, 54. Through Malwarebytes' website, consumers can download free versions of MBAM and Malwarebytes' recently acquired anti-adware product, AdwCleaner. ¶ 58. Malwarebytes also offers a "Premium" MBAM product, which consumers must purchase after a free 14 day-trial to retain full-product functionality. ¶¶ 58-59.

Malwarebytes also markets and promotes its MBAM product through an affiliate program, whereby it pays its affiliates commissions for purchases of MBAM through the affiliates' websites. Bleeping is one of Malwarebytes' affiliates. ¶ 22. On January 5, 2016, ESG filed suit against

[1] To the extent that Malwarebytes attempts to argue ESG is not its competitor, that position is meritless. Both companies provide users with programs that: (1) identify and remediate malware, spyware, trojans, worms, etc.; (2) provide real-time protection to consumers; and (3) are available in a paid, subscription-based format. *See* ¶¶ 46, 49, 54-55, 58-59. Moreover, ESG has alleged the companies are competitors providing similar products in the same market, which must be taken as true in the Rule 12(b)(6) context.

Bleeping in the Southern District of New York, seeking redress for Bleeping's deliberate dissemination of false and misleading information about ESG and SpyHunter (the "Related Case"). ¶¶ 23, 61. As part of Bleeping's smear campaign, it instructed consumers not to install, or to uninstall, SpyHunter and instead purchase MBAM. *Id*. Malwarebytes directly profited from this unlawful conduct and, in fact, provided money to Bleeping for defense costs. ¶¶ 62, 64. ESG served Malwarebytes with a subpoena in the Related Case seeking documents reflecting the nature of Malwarebytes' relationship with Bleeping and the extent of its collaboration with Bleeping to divert sales from ESG to Malwarebytes (the "Subpoena"). ¶¶ 24, 66. Less than a week before Malwarebytes' response to the Subpoena was due, Malwarebytes ***for the first time ever*** began detecting ESG's programs as PUPs and identifying them as "threats" to its users. ¶¶ 25, 72-73. Simultaneously, Malwarebytes publicly announced that it had amended its definition of PUPs to include consideration of "predominantly negative feedback or ratings from the user community," as well as other factors which largely tracked assertions Bleeping made about ESG in the Related Case. ¶¶ 7, 21, 25-27, 67, 71-73.[2]

Once Malwarebytes designated ESG's SpyHunter and RegHunter as PUPs, Malwarebytes' products began blocking consumers' use and installation of ESG's products.[3] ¶¶ 9, 16, 81. For example, for consumers who already have installed and paid for ESG's programs, MBAM "quarantines" the ESG program files as PUPs in a "Total Threats Detected" window, preselects the files for removal, and prompts the user to remove them via a "Remove Selected" button. ¶¶ 82-84. Regardless of whether the user clicks "Remove Selected," MBAM prevents the launch of the ESG programs. ¶ 85. Moreover, even if the user attempts to "Restore" them from MBAM's "Quarantine" window, subsequent attempts by the user to launch the ESG programs will again result in automatic quarantine and failure to launch. ¶¶ 10, 17, 86-89. For customers attempting to

[2] ESG and Bleeping have since settled the Related Case, removing the competitive advantage Malwarebytes enjoyed from Bleeping's smear campaign. *See* Lawrence Abrams, "Press Release," *Bleeping Computer*, available at https://www.bleepingcomputer.com/announcement/bleepingcomputer/press-release/ ("As per a settlement agreement between Bleeping Computer, LLC, and Enigma Software Group USA LLC (ESG), BleepingComputer.com has removed posts written by Quietman7.").

[3] On October 27, 2016, just one week after its acquisition by Malwarebytes, AdwCleaner also began detecting and blocking ESG's programs as PUPs. ¶¶ 13-14.

download ESG's products, MBAM blocks the installer files and prevents the download. ¶ 92. Again, even if a user knows he can "Restore" the quarantined installer files, subsequent attempts to download ESG's programs will result in the same PUP warning and quarantine process. ¶¶ 11, 93-95. As a result, MBAM traps the user in a frustrating and unproductive cycle of attempting to restore or re-download ESG's programs only to have the installer file blocked each and every time. ¶ 95. The only way a user can stop this cycle is to add the files as "Malware Exclusions" (which is counterintuitive because PUPs are not malware), and even if a user knows how to do this, MBAM continues to detect other ESG files as PUPs and threats. ¶¶ 90-91. Malwarebytes' suggestion that it is somehow simple or easy for consumers to whitelist ESG's programs within Malwarebytes' software (*see, e.g.*, Motion, 10, 17) is entirely inaccurate, as the numerous consumer complaints cited in the FAC demonstrate, and in any event, such a factual dispute must be decided in ESG's favor at this stage of the proceedings.

Malwarebytes knows that ESG's programs are legitimate, pose no security threats to a user's computer, and are not harassing in any way. ¶¶ 124-25. Malwarebytes has no objective, good faith basis—because there is none—to claim that ESG's anti-malware programs, which consumers choose to download and purchase, are "potentially unwanted." ¶¶ 18, 126-27. Malwarebytes' "revision" to its PUP criteria was a mere pretense to begin blocking its users' access to ESG's anti-malware programs at its ***malicious whim*** to gain an unfair business advantage, further its anticompetitive scheme and retaliate against ESG for service of the Subpoena. ¶¶ 7-8, 21, 25-27, 67, 72-73, 76, 127. Indeed, a Malwarebytes employee (and developer of AdwCleaner) made the targeted nature of the attack clear in an October tweet that called out ESG but no other company: "#AdwCleaner by @Malwarebytes now fully detects and removes #SpyHunter from Enigma Software Group #PUP." ¶ 78.

By identifying and blocking ESG's anti-malware programs as PUPs, Malwarebytes is falsely representing to the consuming public that ESG's programs, including SpyHunter which competes directly with MBAM, are threats that will compromise computer security if downloaded and/or not removed. ¶ 15. By the time ESG filed the FAC, ESG had received more than 300 consumer

complaints about Malwarebytes' interference with ESG's programs. ¶¶ 101, 123. Certain consumers reported that, although they wanted ESG's programs, they found it impossible or too difficult to exclude them from Malwarebytes' PUP detection process and were, therefore, canceling their ESG accounts, not renewing their subscriptions, and/or wanted refunds of their subscription fees. ¶¶ 101-123, 132. ESG's sales of SpyHunter and RegHunter licenses have already declined and will continue to do so as a result of Malwarebytes' unlawful and predatory anti-competitive conduct. ¶ 131.

ESG originally filed this case in the Southern District of New York. *See* Dkt. 1. There, Malwarebytes moved to dismiss the FAC under Rule 12(b)(2) for lack of personal jurisdiction and Rule 12(b)(6) for failure to state a claim, and in the alternative, to transfer the case to this Court pursuant to 28 U.S.C. § 1404. *See* Dkt. 37-42. On May 12, 2017, Judge Engelmayer granted only the § 1404 motion to transfer for convenience. Op., Dkt. 67, 11. In his Opinion, he expressly "decline[d] to reach the motion to dismiss," including Malwarebytes' personal jurisdiction challenge. *Id.* at 2. Indeed, at the oral argument on the motions, Judge Engelmayer expressed skepticism toward Malwarebytes' claim the Southern District of New York lacked personal jurisdiction over it, asking Malwarebytes' counsel to confirm that Malwarebytes had sales, marketing and customers in New York. *See* Ex. 1, 4:24-6:25.

IV. LEGAL STANDARD

On a Rule 12(b)(6) motion, a court must "take as true all allegations of material fact stated in the complaint and construe them in the light most favorable to the plaintiff." *Watison v. Carter*, 668 F.3d 1108, 1112 (9th Cir. 2012). A motion to dismiss must be denied "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009). Thus, "a complaint need only include enough facts to state a claim that is 'plausible on its face.'" *McKenzie v. Wells Fargo Bank, N.A.*, 931 F. Supp. 2d 1028, 1042 (N.D. Cal. 2013).

V. ARGUMENT

a. Malwarebytes Ignores the Motion to Dismiss Standard.

"[T]he purpose of a motion under Federal Rule 12(b)(6) is to test the formal sufficiency of the statement of the claim for relief; the motion is not a procedure for resolving a contest between the parties about the facts or the substantive merits of the plaintiff's case." 5B Charles Alan Wright & Arthur R. Miller, *Fed. Practice & Procedure* § 1356 (3d ed. 2017). Yet, unable to argue the law in the face of ESG's extensive well-pled allegations, Malwarebytes instead turns to improperly arguing the facts. It makes unsubstantiated claims contradicting ESG's factual allegations and cites evidence extraneous to the FAC, including:

- Claiming as fact its self-serving statement that "Malwarebytes considers many criteria and necessarily updates those criteria as developers change their programs to circumvent Malwarebytes' detection," Motion, Dkt. 97, 8;
- Asserting that ESG's programs were "among several programs that Malwarebytes began blocking as PUPs," even though the FAC paragraphs it cites in support make no reference to ***any*** programs other than SpyHunter and RegHunter, *id.* at 9, and ESG separately pled that "[n]umerous anti-malware products offered by companies other than ESG have been unaffected by Malwarebytes' changed PUP criteria," FAC ¶ 79;
- Claiming that "among other deceptive behavior, Enigma's programs aggressively—and deceptively—identified standard web browser cookies as 'infections' and 'spyware' to scare users into purchasing Enigma software," and "[t]hese deceptive scare tactics exploit consumers' fear about spyware and other threats, even when none exist, to trick them into entering costly subscription plans," Motion, 9, even though ESG's factual allegations state that Malwarebytes knows ESG's programs are legitimate, and not deceptive or aggressive, FAC ¶¶ 124-26;
- Referencing exhibits to the Scott and Newby Declarations, Motion, 9-10, that are not properly subject to judicial notice, *see* Opp. to Request for Judicial Notice, and were filed to improperly seek to refute ESG's well-pled factual allegations;
- Claiming repeatedly that users retain the full ability to configure Malwarebytes' programs to choose whether to keep or remove ESG's programs, Motion, 16, 17, 24, when ESG has, to the contrary, expressly pled that its customers have been unable, or found it too difficult, to exclude ESG's programs from Malwarebytes' willful blocking process, and extensively quoted the myriad cancellation, non-renewal and refund requests from ESG customers who have been unable to prevent blocking of or restore ESG's programs, *e.g.*, FAC ¶¶ 103, 105-06, 109-11, 113-22; and
- Arguing, in a transparent and objectionable attempt to vilify its competitor before this Court, that ESG has "pursued an intimidation campaign for more than a decade of

> threatening and filing lawsuits against security companies that have included SpyHunter in their filters," with the purported effect of "suppressing filtering technologies and reducing consumer control,"[4] Motion, 18, on the basis of exhibits that are not properly subject to judicial notice, *see* Opp. to Request for Judicial Notice, and which, in any event, show only that false detections occur, communications with other companies normally clear up such false positives, but that ESG has on occasion had to resort to the legal system to protect its rights.[5]

If Malwarebytes wishes to rely a factual record, it is welcome to move for summary judgment after discovery. This Court should not permit Malwarebytes to pervert the motion to dismiss procedure, and should disregard Malwarebytes' extensive improper claims and evidence.[6]

b. CDA § 230 Does Not Immunize Malwarebytes from Suit.

Malwarebytes attempts to hide behind the CDA, but the CDA was never intended to and cannot excuse Malwarebytes' unlawful, anti-competitive conduct here. "The CDA was enacted 'to control the exposure of minors to indecent material' on the Internet." *Zango*, 568 F.3d at 1173 (quotation omitted). To further that purpose, CDA § 230(c)(2), entitled "Protection for ***'Good Samaritan'*** blocking and screening of offensive material," provides:

> No provider or user of an interactive computer service ["ICS"] shall be held liable on account of--
>
> > (A) any action voluntarily taken ***in good faith*** to restrict access to or availability of material that the provider or user considers to be ***obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable***, whether or not such material is constitutionally protected; or
> >
> > (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).

47 U.S.C. § 230(c)(2) (emphasis added). Malwarebytes does not, and cannot, contend that ESG's

---

[4] Malwarebytes contradicts its own baseless claim that ESG has "suppressed" filtering technologies and "reduced" consumer control when it claims that "[a]s shown by even a cursory search for Internet security software, consumers have many brands, prices and features from which to choose." Motion, 9.

[5] Malwarebytes conveniently neglects to inform this Court that in every instance it cites of ESG sending cease and desist letters or filing lawsuits, the security companies who had listed ESG as a threat revisited their evaluation, delisted ESG, and do not to list ESG today.

[6] In support of its first motion to dismiss the FAC, Malwarebytes filed a declaration from an employee, Mark Harris, making numerous factual claims intended to refute ESG's allegations, which is impermissible at the pleading stage. Dkt. 39. ESG moved to strike substantial portions of that declaration, Dkt. 46, and to Malwarebytes' credit, it did not refile that declaration in this round of briefing. Accordingly, the claims in that declaration are ***not*** before this Court.

programs are "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing." *Id*. ESG also pled facts showing that its customers want its software and ***choose*** to download those programs, meaning they do not find ESG's programs "objectionable." *See* FAC ¶¶ 17, 48-50. Knowing this, Malwarebytes argues that it is immune from liability under the CDA because ***it unilaterally*** deems a competitor's software, selected by customers, "otherwise objectionable," and because it provides to the customer "technical means to restrict access" to that software. *See* Motion, 13. Malwarebytes is not entitled to immunity for such actions.

1. ESG's Programs Are Not the Types of Materials Addressed by § 230(c)(2).

Malwarebytes glosses over the threshold issue of whether ESG's software is the type of material even covered by the Good Samaritan provision of the CDA. Relying exclusively on the "otherwise objectionable" language, Malwarebytes asserts that it need only "deem" the material somehow objectionable. Motion, 13. Courts, however, have interpreted the term "otherwise objectionable" using the canon of *ejusdem generis* and required before applying the CDA that the content being blocked have some relation to the preceding terms, *i.e.*, the blocked content has some element of being "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing." *See Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883 (N.D. Cal. 2015) ("[W]hen a statute provides a list of examples followed by a catchall term (or 'residual clause') like 'otherwise objectionable,' the preceding list provides a clue as to what the drafters intended the catchall provision to mean. … Given the list preceding 'otherwise objectionable,'—"obscene, lewd, lascivious, filthy, excessively violent, [and] harassing ...'—it is hard to imagine that the phrase includes, as YouTube urges, the allegedly artificially inflated view count associated with 'Luv ya.'" (internal citations omitted)); *Goddard v. Google, Inc.*, 08-2738, 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008); *Nat'l Numismatic Certification, LLC v. eBay, Inc.*, 08-42, 2008 WL 2704404, at *25 (M.D. Fla. July 8, 2008) (rejecting argument "that Congress intended the general term 'objectionable' to [immunize restricting access to] an auction of potentially-counterfeit coins" because "the word ['objectionable'] is preceded by seven other words that describe pornography, graphic violence, obscenity, and harassment").

Because the types of materials defined in Malwarebytes' PUP criteria, and specifically ESG's programs, are not remotely related to the content categories enumerated in the CDA,[7] Malwarebytes is not entitled to CDA immunity. *See Song fi*, 108 F. Supp. 3d at 883 ("[E]ven if the Court can 'see why artificially inflated view counts would be a problem for ... YouTube and its users,' … the terms preceding 'otherwise objectionable' suggest Congress did not intend to immunize YouTube from liability for removing materials from its website simply because those materials pose a 'problem' for YouTube." (internal citations omitted)); *Goddard*, 2008 WL 5245490, at *6 ("[T]he relevant portions of Google's Content Policy require that MSSPs provide pricing and cancellation information regarding their services. These requirements relate to business norms of fair play and transparency and are beyond the scope of § 230(c)(2).").

Malwarebytes attempts to escape this conclusion by wrongly asserting *Zango* decided this issue, purportedly allowing a company to, completely unmoored from "some independent standard," deem a competitor's software "objectionable." Motion, 13. But unlike here, in *Zango*, the plaintiff ***waived*** any argument on appeal that its "software is not 'otherwise objectionable' under § 230(c)(2)." 568 F.3d at 1178 (Fisher, J., concurring). In fact, the Court specifically observed that "[b]ecause Zango has not argued that the statute limits the material a provider of an interactive computer service may properly consider 'objectionable,' that question is not before us." *Id.* at 1177 n.8. Thus, *Zango* did not hold that § 230(c)(2) incorporates no independent standard, and in fact expressly disclaimed any such holding. To the extent the arguments at issue here were addressed in *Zango* at all, it was Judge Fisher that commented on them in ESG's favor in his concurrence, indicating that *Zango* did not grant companies an unfettered license to attack competitors' products on a whim with anticompetitive, harmful tactics and to hurt consumers' right to choose products of

[7] Malwarebytes asserts that because its PUP criteria includes "excessive or deceptive distribution, affiliate or opt-out bundling practices" and "aggressive or deceptive behavior especially surrounding purchasing or licensing," it "cannot be disputed that Malwarebytes considers PUPs that exhibit these features to be objectionable, in a way that is similar to the adware at issue in *Zango* and 'harassing' spam emails at issue in *Holomaxx*." Motion, 14. Yet Malwarebytes never claims ESG's programs satisfy those particular criteria. And Malwarebytes never explains—because there is no plausible explanation—how the amorphous distribution, purchasing or licensing practices referenced in its PUP policy are harassing or a form of adware. Finally, ESG expressly pled that Malwarebytes does not actually consider ESG's programs to be harassing, otherwise objectionable, or a threat, so any of Malwarebytes' claims to the contrary are inappropriate on a motion to dismiss. *See* FAC, ¶¶ 124-25.

their own choice.

2. ESG Sufficiently Pleads that Malwarebytes Has Not Acted in "Good Faith."

Malwarebytes recognizes that it is not entitled to immunity under subsection A of § 230(c)(2) if it failed to act in "good faith," but improperly disregards ESG's factual allegations that it did just that. The FAC alleges that just one week before Malwarebytes was required to respond to the Subpoena regarding its involvement in Bleeping's unlawful conduct to divert sales from ESG to Malwarebytes, it revised its PUP criteria to "interfer[e] with ESG's current and prospective customer base, injur[e] ESG's business, and retaliat[e] against ESG[.]"[8] FAC ¶¶ 7-8, 25. ESG also alleges that Malwarebytes had never before detected ESG's programs as PUPs and the revised criteria were created to target ESG's programs and track defenses asserted by Bleeping in the Related Case to assist in Bleeping's defense. ¶¶ 6, 25-27, 75. Finally, the FAC alleges that "Malwarebytes has no objective, good faith basis to claim that ESG's products are" PUPs and that the consumer complaints quoted in the FAC establish that "customers who have already downloaded (and paid for), or are trying to download, SpyHunter or RegHunter ***want*** those programs on their computer, a fact Malwarebytes knows." ¶ 126 (original emphasis).

Malwarebytes argues that if competition had motivated it to change its PUP criteria, it "would have made those changes … earlier in the seven years that Malwarebytes and SpyHunter have coexisted." Motion, 17. Malwarebytes, however, held a significant competitive advantage over ESG by way of Bleeping's unlawful conduct which it has now lost because the Related Case settled. *See supra* at n.1. Malwarebytes' decision to begin detecting ESG's programs as PUPs at the

[8] Malwarebytes misunderstands ESG's allegations when it argues that the fact that it changed its PUP criteria "approximately *nine months* after [ESG] sued Bleeping … flatly contradicts [ESG's] theory that Malwarebytes' update of its PUP criteria was a retaliatory move, in bad faith." Motion, 19 (original emphasis). The FAC alleges that Malwarebytes changed its PUP criteria in retaliation against ESG for ***ESG's service on Malwarebytes of a Subpoena*** to produce documents in the Bleeping case. ¶¶ 21, 24, 72. Certainly, this chronology creates a plausible inference that Malwarebytes did not act in good faith. Malwarebytes does nothing more than claim, in a single sentence, that "Plaintiff's allegation that Malwarebytes revised its PUP criteria in retribution for being served with a subpoena in the Bleeping case is unsupported speculation." Because ESG's well-pled factual allegations must be taken as true and it is entitled to reasonable inferences therefrom, this Court should ignore Malwarebytes' conclusory rebuttal.

time its Subpoena response was due—*i.e.*, at the time it was forced to recognize the seriousness of ESG's suit against Bleeping and the imminent loss of its competitive advantage—gives rise to a plausible inference that Malwarebytes began detecting and blocking ESG's programs as PUPs to retaliate against and harm ESG. Moreover, that Malwarebytes never before detected ESG's programs as PUPs (FAC ¶ 6) shows that Malwarebytes does not ***actually*** find ESG's programs "objectionable"—if it did, it would have begun to detect and block them years ago—and its revised PUP policy is merely a pretext for anticompetitive action.

The remainder of Malwarebytes' arguments are entirely irrelevant. For example, Malwarebytes argues that ESG "does not refute that its software meets one or more of the [PUP] criteria, or that those criteria are not proper measures of PUPs." Motion, 16. While the FAC taken as a whole clearly disputes those points, whether ESG's programs meet Malwarebytes' PUP criteria has no bearing on whether Malwarebytes established those criteria without a good faith basis and to retaliate against and harm ESG. Similarly, whether any of the PUP criteria would result in identification of actual PUPs—which ESG's programs are not (FAC ¶ 124)—has no bearing on whether Malwarebytes implemented those criteria in bad faith and to target ESG. In short, the FAC sets forth clear allegations that go far beyond the specificity required under the applicable notice-pleading standards[9] and support a plausible inference that Malwarebytes' detection and blocking of ESG's programs as PUPs was not undertaken in good faith. Malwarebytes and other malware providers are free to develop and distribute, in good faith, consumer protective filtering technologies

[9] Given the specificity of ESG's allegations, Malwarebytes' citations to *Holomaxx Tech. v. Microsoft Corp.*, 783 F. Supp. 2d 1097 (N.D. Cal. 2011), and *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008), as alleged support for its "good faith" argument are misplaced. In *Holomaxx*, plaintiff did not plead—as ESG pleads here—that defendant designed its "filtering technologies" specifically to target plaintiff in retaliation or to cause it harm. *Id*. at 1105. Rather, plaintiff pled "conclusorily that [defendant] acted in bad faith," alleging only that defendant was "'[p]ossibly seeking to cut costs in its free email service' and … on information and belief … profit[ed] from requiring senders to join 'whitelists[.]'" *Id*. In *e360Insight*, plaintiff did not plead ***any*** facts giving rise to a plausible inference of the absence of defendant's good faith. 546 F. Supp. 2d at 609. For this reason, the Court rejected plaintiff's argument that defendant acted in bad faith when it "allow[ed] numerous other companies to send bulk e-mails in greater volume and with greater frequency … singling out Plaintiff when other behaving in a like manner are not treated in a like fashion." *Id*. (also noting that Comcast did not claim that it refused to transmit e360's electronic mails because of "their volume and their frequency").

that target software that actually is fake, deceptive or malicious. *See* Motion, 17-18. They may not, however, target competitors with demonstrably false allegations and prohibit their competitors' customers from using the software they want.

Indeed, in the *Zango* case that Malwarebytes heavily relies on, Judge Fisher expressed the identical point on the proper limits of the CDA. He explained that the CDA was not intended to and should not extend immunity to a party that "abuse[s] the immunity" by unilaterally "block[ing] content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material 'otherwise objectionable.'" 568 F.3d at 1178 (Fisher, J., concurring). He further explained that the CDA should not protect a party who abuses the CDA by being "less accommodating to the user's preferences" either by "not providing an override option or making it difficult to use." *Id.*

Judge Fisher's concerns apply in full force to Malwarebytes' blocking of ESG's software. The FAC alleges facts showing that Malwarebytes revised its PUP criteria as a pretense to begin blocking its users' access to ESG programs at its malicious whim for anti-competitive purposes. FAC ¶¶ 7-8, 21, 25-27, 67, 72-73, 76, 127. Additionally, Malwarebytes does ***not*** enable ESG's customers to continue (or begin) using ESG's programs, even though they want to, frequently have already paid to, and have complained to Malwarebytes about the unjustified blocking. Indeed, many users cannot override Malwarebytes' designation of ESG's products as PUPs and that quarantines and blocks prevent access to and use of ESG's products. *E.g.*, ¶¶ 11, 88-95, 103, 105-06, 109-11, 113-22. Thus, extending immunity to Malwarebytes for its unilateral, bad faith, anti-competitive blocking of ESG's programs would be an abuse of the immunity intended by Congress "to facilitate users' access to blocking software that makes Internet use 'safer' than it otherwise would be." *Zango*, 568 F.3d at 1179 (Fisher, J., concurring).

3. § 230(c)(2)(B) Does Not Save Malwarebytes' Claim to Immunity.

When Malwarebytes first moved to dismiss the FAC, it correctly recognized that good faith was a requirement across both subsections of § 230(c)(2). *See* Mem. in Supp. of Mot., Dkt. 38, 24 ("A plaintiff asserting a claim against a provider of filtering software bears the burden of proving

that a provider failed to act in good faith."). Now, despite relying primarily on the same cases in this renewed Motion, Malwarebytes has done an about-face, newly contending that § 230(c)(2)(B) does not require good faith. Subsection (B), however, provides no immunity to Malwarebytes for two independent reasons.

First, Malwarebytes' claim to immunity under subsection (B) fails because ESG's programs are not the type of material covered by § 230(c)(2). Subsection (B) provides immunity for "any action taken to enable or make available … the technical means to restrict access to the materials described" in subsection (A)—*e.g.* "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[10] Thus, immunity under subsection (B) exists only for technical means that block the enumerated materials. As set forth above in Section V.a.1, ESG's programs do not fall within those enumerated materials, and thus Malwarebytes' actions fall outside the scope of subsection (B).

Second, good faith is an implied requirement in subsection (B) that is part and parcel of the proper, plain meaning of the statute when read as a whole. While it is true that only subsection (A) explicitly requires that an "action" "to restrict access" be taken in "good faith," the structure of the section necessarily applies the "good faith" requirement more broadly. It would be logically impossible for an entity to take an "action" in *good* faith "to restrict access" to "material," if it had in *bad faith* deemed that material to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." In turn, because the entity must in *good* faith consider material to satisfy one of subsection (A)'s enumerated categories, the entity could not then in turn under Subsection (B) "enable or make available … the technical means to restrict access" to that material in *bad* faith. Thus, Subsection (B) requires that Malwarebytes act in good faith, and as set forth above in Section V.a.2, ESG has adequately pled that Malwarebytes has not done so, overcoming any potential immunity.

[10] Although the statutory text references "material described in paragraph (1)," this is "a typographical error, and … instead the reference should be to paragraph (A), i.e., § 230(c)(2)(A)." *Zango*, 568 F.3d at 1173 n.5.

4. ESG's Lanham Act Claim is Not Subject to the CDA.

Even if §230(c)(2) immunity was available to Malwarebytes, which it is not, it would ***not*** bar ESG's Lanham Act claim. Section 230(e)(2) provides that "nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). "[O]n the basis of th[is] statutory text, … the CDA does not bar [a § 43(a)] Lanham Act claim." *Enigma Software Grp. USA v. Bleeping Computer LLC*, 194 F. Supp. 3d 263, 273-74 (S.D.N.Y. 2016) (citing *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001)); *see also Gen. Steel Dom. Sales, LLC v. Chumley*, 14-CV-01932-REB-CBS, 2015 WL 4911585, at *9 (D. Colo. Aug. 18, 2015), *appeal dismissed sub nom. Gen. Steel Dom. Sales, L.L.C. v. Chumley*, 840 F.3d 1178 (10th Cir. 2016) ("The § 1125 [false advertising] claim of the plaintiff is an intellectual property claim. Therefore, this claim does not fall within the ambit of § 230 immunity claimed by the defendants."); *Nieman v. Versuslaw, Inc.*, 12-3104, 2012 WL 3201931, at *8 (C.D. Ill. Aug. 3, 2012), *aff'd*, 512 Fed. Appx. 635 (7th Cir. 2013) ("[T]he Lanham Act claim would most certainly be considered an intellectual property claim.").[11]

c. ESG Sufficiently Pleads Violations of the Lanham Act and NYGBL.

Like its failed immunity argument, Malwarebytes' arguments that ESG's Lanham Act and NYGBL claims should be dismissed for failing to allege an actionable "false or misleading statement" or "commercial advertising or promotion" (Motion, 19-22) must fail.

1. ESG Sufficiently Pleads Actionable "False and Misleading Statements."

Malwarebytes' detection and blocking of ESG's programs as PUPs is ***not***, as Malwarebytes' contends, non-actionable opinion for the following three reasons. Motion, 19-21. ***First***, the context of the statements as alleged in the FAC plausibly supports the conclusion that consumers would understand the statements as ones of fact, not opinion. Malwarebytes is a self-professed leader in the anti-malware and Internet security industry (FAC ¶ 3) and, through its programs and forums, informs

[11] Malwarebytes cites only two cases in support of its contrary position, but neither are apposite. *Zango* addresses only torts, not the statutory violations set forth in the Lanham Act. 568 F.3d at 1177. *Associated Bank-Corp. v. Earthlink, Inc.*, 05-233, 2005 WL 2240952, at *4 (W.D. Wis. Sept. 13, 2005), on the other hand, did grant Section 230 immunity for a series of claims, including injunctive relief under the Lanham Act, but did not consider or address the reach of Section 230(e)(2)'s intellectual property law exemption.

the consuming public, including novice computer users, that ESG's programs are potential threats to computer security.[12] As evidenced by the consumer complaints quoted in the FAC, consumers understand this statement by Malwarebytes to be fact.

Second, it is entirely irrelevant that Malwarebytes detects and blocks ESG's programs as "***potentially***" unwanted. Motion, 21. The word "potentially" does not make Malwarebytes' misrepresentations any less susceptible to proof of falsity.[13] Nor does it make Malwarebytes' misrepresentations any less likely to mislead consumers. Indeed, consumers plausibly would be influenced not to do business with ESG based on the mere suggestion that ESG's programs might threaten computer security or should be "unwanted."

Third, ESG alleges that Malwarebytes is ***intentionally*** misleading consumers by representing that ESG's programs are PUPs when, in reality, Malwarebytes ***knows*** ESG's programs are ***not*** PUPs. *Abu Dhabi Commercial Bank v. Morgan Stanley & Co. Inc.*, 651 F. Supp. 2d 155 (S.D.N.Y. 2009) ("[A]n opinion may still be actionable if the speaker ***does not genuinely and reasonably believe it*** or if it is ***without a basis in fact***.") (emphasis added). Not a single one of Malwarebytes' cited cases involved allegations—as ESG makes here—that defendants ***knew*** their representations were false when made.

2. ESG Sufficiently Pleads "Commercial Advertising and Promotion."

Malwarebytes also argues that "[o]nly *existing* users of [its] software would see the detection of [ESG's] programs as PUPs" and, therefore, the FAC does not allege "commercial advertising or promotion" sufficient to support ESG's Lanham Act claim. Motion, 21-22 (original emphasis). This is false. ESG alleges Lanham Act liability based, in part, on Malwarebytes' false statements about ESG's programs on its website, which is available to the consuming public generally, not just

[12] At a minimum, the representations are actionable "mixed opinions." *See Steinhilber v. Alphonse*, 68 N.Y.2d 283, 289 (N.Y. Ct. App. 1986) ("[When a] statement of opinion implies that it is based upon facts which justify the opinion but are unknown to those reading or hearing it, it is a 'mixed opinion' and is actionable. The actionable element of a 'mixed opinion' is not the false opinion itself--it is the ***implication that the speaker knows certain facts***, unknown to his audience, ***which support his opinion*** and are detrimental to the [party] about [which] he is speaking.") (emphasis added) (citations omitted).

[13] Indeed, in its simplest form, the statement that a dog is "potentially" a cat can certainly be proven false.

Malwarebytes' existing customers. *E.g.*, FAC ¶ 158 (alleging liability based on "Malwarebytes' false and misleading statements … shown to the consuming public, ***including persons not currently using MBAM and/or AdwCleaner***, via various threads on the Forums webpage of Malwarebytes' website and via the public announcement on Twitter").[14] In fact, a Malwarebytes "Elite Member" posted on Malwarebytes' Forums webpage that Malwarebytes' programs now detect ESG's programs as PUPs, *i.e.*, "programs that come[] bundled with some extra unwanted crap," and asked: "Anyway, ***why use SpyHunter when you have Malwarebytes?***" ¶ 96 (emphasis added). Malwarebytes cannot seriously contend that this is not "disseminat[ion] to the relevant purchasing public" of statements aimed at "influencing consumers to buy" its products. Motion, 21. Thus, the Court should deny the Motion to dismiss ESG's Lanham Act and NYGBL claims.

d. ESG Sufficiently Pleads Tortious Interference.

1. New York Law Applies to ESG's Claims.

Malwarebytes asks this Court to apply California law to ESG's tortious interference claims on its bare say-so that the Southern District of New York lacked personal jurisdiction over Malwarebytes. *See* Motion, 23 ("Because Malwarebytes maintains that the Southern District of New York lacked personal jurisdiction and that transfer to this district cures the defect in personal jurisdiction, this Court should apply California law to Enigma's common law claims."). Yet Malwarebytes fails to (i) make any argument as to why that district lacked personal jurisdiction, (ii) provide even a shred of evidence to this Court to support its position, or (iii) even incorporate by reference its prior briefing to the Southern District of New York on this issue. Accordingly, Malwarebytes has waived any argument that California law should apply because the Southern District of New York lacked personal jurisdiction over it. *See John-Charles v. Cal.*, 646 F.3d 1243,

[14] Malwarebytes further grasps at straws when arguing that its baseline MBAM product is free and thus its false statements about ESG's products were not made "for the purpose of influencing consumers to buy" Malwarebytes' programs." Motion, 24. That argument is illusory. Malwarebytes sells a "Premium" MBAM product that has five distinct technical capabilities that, in its free product, expire after the first 14 days of use. FAC ¶¶ 58-59. It is plausible, as alleged in the FAC, that "Malwarebytes' intention in offering its free MBAM and AdwCleaner downloads is to preview its products' capabilities and entice consumers to ultimately purchase the Premium MBAM product." ¶ 60 ("[T]he free MBAM and AdwCleaner downloads are marketing tools for Malwarebytes."). It is irrelevant that the FAC does not allege that the "PUP detection and removal features expire." Motion, 24.

1247 (9th Cir. 2011) ("John–Charles has failed to develop any argument on this front, and thus has waived it."); *U.S. v. Ramirez*, 448 Fed. Appx. 727, 729 (9th Cir. 2011) (unpublished) ("Ramirez stated in conclusory terms that the district court violated his due process rights, but he did so in a single sentence without citation to authority. An undeveloped argument of this sort is waived."); *U.S. v. Romm*, 455 F.3d 990, 997 (9th Cir. 2006) ("[A]rguments not raised by a party in its opening brief are deemed waived").

Even if Malwarebytes had not waived this argument, it would still fail because personal jurisdiction over Malwarebytes existed in the Southern District of New York. Notably, despite filing two briefs, several declarations and a request for judicial notice in the Southern District of New York, and another brief, two declarations and a request for judicial notice in this Court, Malwarebytes still has not even attempted to put forth any facts to refute or attempt to deny that:

- Malwarebytes generates revenues from sales to New York consumers;
- it employs residents, including as sales representatives, in New York;
- New York consumers visit and interact with its website and forum webpages;
- New York consumers download and purchase its MBAM and AdwCleaner programs from its website; and
- its MBAM and AdwCleaner programs have detected and blocked ESG's programs as PUPs and "threats" on the computers of New York consumers.

FAC, ¶¶ 37-40, 42-43, 104, 107, 112, 117-18, 121-23. These allegations are legally sufficient to establish personal jurisdiction. First, personal jurisdiction exists under CPLR § 302(a)(1), "a '***single act***' statute, under which 'proof of ***one transaction*** in New York is sufficient to invoke jurisdiction, even though the defendant never enters New York, so long as the defendant's activities here were purposeful and there is a substantial relationship between the transaction and the claim asserted." *Pearson Educ., Inc. v. Shi*, 525 F. Supp. 2d 551, 555 (S.D.N.Y. 2007) (emphasis added, citations omitted). Malwarebytes purposefully and wrongfully detects and blocks ESG's programs as PUPs and "threats" ***on consumers' devices***, thereby falsely advertising and tortiously interfering with ESG's business. Such conduct indisputably occurred in New York, and establishes jurisdiction.[15]

[15] Malwarebytes cannot argue that it did not "target" New York customers, because Malwarebytes cannot dispute that New York consumers have, through its website, downloaded and purchased Malwarebytes products that identify ESG's programs as PUPs. "[O]ne who uses a web site to make sales to customers in a distant state can thereby become subject to the jurisdiction of that state's courts." *Student Advantage, Inc. v. Int'l Student Exch. Cards, Inc.*, 00-1971, 2000 WL 1290585, at

Second, Malwarebytes is subject to jurisdiction under CPLR § 302(a)(3) because ESG has sufficiently alleged that Malwarebytes committed a tortious act outside of New York that has "caus[ed] injury" to a person in New York.[16] Indeed, the FAC extensively quotes the cancellation, non-renewal and refund requests ESG has received from its customers residing in New York who were unable to use ESG's programs and/or unable to restore them from quarantine because of Malwarebytes' false and misleading identification of the programs as PUPs. *See* FAC ¶¶ 104, 107, 110, 112, 117-18, 121-23.

Because Malwarebytes was subject to personal jurisdiction in the Southern District of New York, this Court should continue to apply New York law to ESG's tortious interference claims. *See Schering Corp. v. First DataBank Inc.*, 07-1142, 2007 WL 1176627, at *3 (N.D. Cal. Apr. 20, 2007) (requiring the transferee court to apply transferor court's law "[w]hen a case is transferred on grounds of convenience pursuant to 28 U.S.C. 1404(a)").

2. ESG Has Stated A Claim for Interference With Prospective Economic Advantage.

Malwarebytes mounts only two challenges to ESG's pleading of interference with prospective business advantage under either New York or California law, but both challenges fail.[17] ***First***, Malwarebytes incorrectly claims that "Enigma fails to plausibly allege that Malwarebytes

*4 (S.D.N.Y. Sept. 13, 2000) (finding personal jurisdiction proper where defendant's website was "accessible" to New York consumers and "require[d] the purchaser to exchange [payment and shipping] information with [defendant] via the internet").

16 Section 302(a)(3) also requires that the non-domiciliary either (i) "regularly does or solicits business … or derives substantial revenue from goods used … or services rendered[] in" New York, or (ii) "should reasonably expect the act to have consequences in [New York] and derives substantial revenue from interstate or international commerce." Malwarebytes does not, and cannot, argue that ESG has failed to sufficiently allege these facts. *E.g.*, FAC ¶ 39.

17 Under New York law, for tortious interference with prospective economic advantage, a plaintiff must plead that "(1) it had a business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship." *Kirch v. Liberty Media Corp.*, 449 F.3d 388, 400 (2d Cir. 2006). Similarly, under California law, for intentional interference with prospective economic advantage, the plaintiff must plead "(1) the existence, between the plaintiff and some third party, of an economic relationship that contains the probability of future economic benefit to the plaintiff; (2) the defendant's knowledge of the relationship; (3) intentionally wrongful acts designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm proximately caused by the defendant's action." *Roy Allan Slurry Seal, Inc. v. Am. Asphalt S., Inc.*, 388 P.3d 800, 803 (Cal. 2017).

intentionally disrupted Plaintiff's prospective economic relationship through some wrongful or tortious conduct." Because Malwarebytes' violations of the Lanham Act and NYGBL are independent torts and ESG sufficiently pleads those claims, the FAC sufficiently pleads "wrongful means." *See Sidney Frank Importing Co., Inc. v. Beam Inc.*, 998 F. Supp. 2d 193, 211–12 (S.D.N.Y. 2014) (noting "wrongful means" exist where, *inter alia*, the defendant's conduct is an "independent tort"); *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P. 3d 937, 954 (Cal. 2003) ("[A]n act is independently wrongful if it is unlawful, that is, if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard."). Moreover, the FAC pleads that Malwarebytes "engage[d] in conduct for the sole purpose of ***inflicting intentional harm*** on" ESG, *i.e.*, that Malwarebytes revised its PUP criteria for the purpose of "interfering with ESG's current and prospective customer base, injuring ESG's business, and retaliating against ESG" for its service of a Subpoena in the Related Case. FAC ¶¶ 7-8, 25-27; *Sidney Frank*, 998 F. Supp. 2d at 211–12 (noting "wrongful means" exist where, *inter alia*, defendant's conduct is undertaken "for the sole purpose of inflicting intentional harm" on the plaintiff). Malwarebytes' argument that there can be no "wrongful conduct" because Malwarebytes "expresses its opinion that programs are PUPs" but "the users ultimately decide whether to install and purchase Enigma's program" is fatally flawed, both factually and legally. Motion, 24. It is plausible that a consumer considering use of one of ESG's programs would choose not to do business with ESG due to concerns about the program's legitimacy because Malwarebytes detects and blocks the program as a PUP. It is also plausible that a consumer would become so frustrated with Malwarebytes' repeated detection and blocking of ESG's programs that they would choose not to do business with ESG. Malwarebytes' suggestion that consumers can easily use both programs contemporaneously is belied by the allegations of the FAC and must be rejected at the motion to dismiss phase.

Second, Malwarebytes erroneously claims ESG has not identified "prospective customers with whom Malwarebytes interfered" or pled "that Malwarebytes knew about [ESG's] prospective economic relationship with those … customers." Motion, 24. This is plainly belied by ESG's allegations, which make clear that Malwarebytes interferes with each prospective ESG customer

who has Malwarebytes' anti-malware program installed, attempts to obtain ESG's programs, and is prevented from downloading, installing, and using them by Malwarebytes' anti-malware program. *See, e.g.*, FAC ¶¶ 8-10, 81-95, 162-65. Malwarebytes knows such prospective customers exist, or it would not have bothered identifying ESG's programs as PUPs. *See Reading Intern., Inc. v. Oaktree Capital Mgmt. LLC*, 317 F. Supp. 2d 301, 335 (S.D.N.Y. 2003) (holding it "would be unreasonable to require" plaintiff to identify specific contracts lost "prior to discovery"); *Silicon Valley Test & Repair, Inc. v. Gen. Signal Corp.*, 93-20448, 1993 WL 373977, at *5 (N.D. Cal. Sept. 13, 1993) (finding intentional interference adequately pled where plaintiff alleged defendants "interfered with prospective economic advantages between [plaintiff] and certain of its customers and potential customers on a repeated basis" and noting plaintiff "was not required to plead with the particularity Defendants demand" because "Defendants can obtain the details through discovery").

3. ESG Has Stated A Claim for Interference With Contractual Relations.

Malwarebytes contests the adequacy of ESG's allegations of interference with contractual relations on the basis that ESG has not alleged a "valid contractual obligation that was breached or disrupted."[18] Motion, 25. In so claiming, Malwarebytes again improperly ignores ESG's well-pled factual allegations. ESG has asserted that it has (i) contractually licensed the SpyHunter and RegHunter software to numerous customers and (ii) certain of those customers, after encountering Malwarebytes' block on ESG's programs, requested refunds and/or cancelled their subscriptions despite having used and been otherwise satisfied with ESG's programs. FAC ¶¶ 101, 105-06, 109, 111, 116, 118-20, 123, 132, 152, 159. This is sufficient to plead a breach. *See Nat. Res. Media &*

[18] Under New York law, tortious interference with contractual relations requires "(1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of the contract; (3) the defendant's intentional procurement of the third-party's breach of the contract without justification; (4) actual breach of the contract; and (5) damages …." *Kirch*, 449 F.3d at 401 (internal quotations omitted). Similarly, under California law, intentional interference with contractual relations requires "(1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of that contract; (3) the defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage." *Reeves v. Hanlon*, 95 P.3d 513, 517 (Cal. 2004). Unlike interference with prospective economic advantage, this tort does not require an independently wrongful act. *See Gym Door Repairs v. Young Equip. Sales*, 206 F. Supp. 3d 869, 908 (S.D.N.Y. 2016); *Quelimane Co. v. Stewart Title Guar. Co.*, 960 P.2d 513, 530 (Cal. 1998), *as modified* (Sept. 23, 1998).

Tech. Grp., LLC v. Snoop Youth Football League Found., 07-7701, 2008 WL 728650, at *3 (S.D.N.Y. Mar. 14, 2008) (holding, for interference with contract claim, that complaint language stating third party "withdrew" and "served written notice of cancellation" was "synonymous with a breach"). Moreover, contrary to Malwarebytes' assertion, California law "does not necessarily require evidence of any 'breach'"; rather, there need be only a ***disruption***, which exists where a defendant's "intentional actions resulted in greater expense or burden on the performance of [plaintiff's] contractual obligations with third parties." *Sebastian Intern., Inc. v. Russolillo*, 162 F. Supp. 2d 1198, 1204-05 (C.D. Cal. 2001); *Almont Ambulatory Surgery Ctr., LLC v. UnitedHealth Grp., Inc.*, 121 F. Supp. 3d 950, 982 (C.D. Cal. 2015). It cannot be reasonably disputed that providing refunds makes fulfillment of a contract more expensive, or that fielding complaints and requests to technical support staff to address Malwarebytes' block makes fulfillment of a contract more burdensome.[19]

CONCLUSION

ESG respectfully requests that the Court deny in its entirety Malwarebytes' Motion.

Dated: October 6, 2017

Respectfully submitted,

K&L GATES LLP

By: */s/ Edward P. Sangster*
Edward P. Sangster
Terry Budd
Christopher M. Verdini
Anna Shabalov

Attorneys for Plaintiff

[19] In passing, Malwarebytes also makes the conclusory claim that ESG supposedly did not allege that Malwarebytes intentionally sought to induce a breach. Motion, 26. Yet again, Malwarebytes overlooks ESG's well-pled factual allegations: (i) "Malwarebytes knows that users who have SpyHunter and/or RegHunter installed on their computers, or who are seeking to download and install SpyHunter and/or RegHunter, contractually license that software from ESG" and (ii) "Malwarebytes has intentionally and maliciously … induced users to choose not to install SpyHunter and RegHunter or to delete SpyHunter and RegHunter and … disabled SpyHunter and RegHunter programs that ESG customers have already paid to install and use, causing confusion and anger among ESG's customers." FAC, ¶¶ 156-57.

EXHIBIT 1

EXHIBIT 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

ENIGMA SOFTWARE GROUP USA, LLC,

Plaintiff,

v. 16 Civ. 7885 (PAE)

MARLWAREBYTES INC.,

Argument

Defendant.

----------x

New York, N.Y.
February 3, 2017
2:15 p.m.

Before:

HON. PAUL A. ENGELMAYER

District Judge

APPEARANCES

K&L GATES LLP
Attorneys for Plaintiff
BY: TERRY BUDD
CHRISTOPHER M. VERDINI
ERIC A. PRAGER

FENWICK & WEST LLP
Attorneys for Defendant
BY: TYLER G. NEWBY

(Case called)

THE COURT: Good afternoon to you. You may all be seated. We are here for oral argument on the pair of motions that Malwarebytes has made to either dismiss the case or, alternatively, transfer it.

Before we begin the argument, there has been, as counsel at least at the front table know, a development in the other case that I am hearing that involves overlapping events and issues. I don't know whether Malwarebytes is aware of this, but I received a letter yesterday from Enigma reporting a settlement in principle between Enigma and Bleeping. On the strength of that, I had issued a so-called 30-day order that discontinues the case without prejudice to the right of either party in that case to ask that the case be reactivated if the process of finalizing settlement terms isn't accomplished within that time period.

What does that mean for this case, Enigma? Mr. Verdini.

MR. VERDINI: Yes, your Honor. I don't think it means anything for this case.

THE COURT: I don't want to know the substance, but there were not, I take it, parallel settlement discussions between Enigma and Malwarebytes?

MR. VERDINI: No, there weren't, your Honor.

THE COURT: From your perspective, there are no

implications for this case from the fact that the case that originally led this to be treated as a related case before me is now apparently going away?

MR. VERDINI: Correct. We think venue is still proper. We still have jurisdiction over Malwarebytes here.

THE COURT: I understood that. That would have been the case regardless of whether the case was factually related; you still would have had to prove those things.

MR. VERDINI: Correct.

THE COURT: What I mean is right now this was not part of some effort to achieve a global settlement.

MR. VERDINI: You are correct, your Honor. It was just with Bleeping.

THE COURT: It is what it is. Very good.

MR. VERDINI: Your Honor, we did email a copy to Mr. Newby of the letter that we sent so that he was aware of the settlement in case it affected his argument today.

THE COURT: Good to know. Thank you. I appreciate you're doing that.

Mr. Newby, I will hear from you briefly.

MR. NEWBY: Your Honor, thank you. I would like to address two principal points, first on the motion to transfer, the motion for personal jurisdiction. Secondly, I would like to focus on the Communications Decency Act argument. If your Honor has any preference?

THE COURT: Let's take the transfer issue first.

MR. NEWBY: Although plaintiffs did not make it a principal part of their argument for the relatedness of this case to this district, I think the settlement or pending settlement in the Bleeping matter makes this district all the more attenuated in its in connection with the dispute between Malwarebytes and Enigma.

The principal issue here is that Malwarebytes over time has developed and refined its criteria for blocking or filtering the potentially unwanted programs. This has gone on for many years. In October it updated those criteria to include Enigma's software, the Spyhunter and Reghunter software. All of that work and all the witnesses as to the rationale for doing that, all of that took place in California.

The servers by which all of the consumers who use Malwarebytes software on their computers throughout the world, throughout the country, those computers connect to servers in California. That's where they get the definition updates. That would include the Enigma software blocking.

Really all of the events, the locus of events is in California. Malwarebytes doesn't have an office here. It has a handful of employees who work remotely, but they work on enterprise sales, which is not the focus of this case.

THE COURT: You do have sales in New York though?

MR. NEWBY: The company does have customers in New

York, yes, your Honor. There are two strains, I should say three strains of Malwarebytes software. There is the free version that anybody can download and use. There is a premium version that users will pay for additional features. Then there is an enterprise version. The enterprise version is where sales are actually focused on particular customers. Those would be businesses.

As per Mr. Harris's declaration, for the consumer software, which is really the focus of this case, there is no direction toward New York. There is no directed or concerted sales activity marketing toward New York.

THE COURT: Is there marketing on the enterprise version?

MR. NEWBY: Yes, there is, your Honor.

THE COURT: You're saying that the software feature that is at issue in this case literally is absent from the enterprise version?

MR. NEWBY: No, your Honor, it would be present. Based on the allegations of the complaint, as we understand it --

THE COURT: I'm not sure I'm following. In other words, are you saying that there is no circumstance where software that has the allegedly offending features is being sold to customers in New York?

MR. NEWBY: There would be situations for the

enterprise software where it would be sold to customers located in New York.

THE COURT: Right.

MR. NEWBY: Also, if there are customers, individual consumers, who are using the consumer version, which is the focus of this lawsuit --

THE COURT: Is enterprise out of the bounds of this lawsuit or is the consumer the larger part of this lawsuit?

MR. NEWBY: We certainly do not read the allegations of the complaint to address the enterprise software. The premier version of the consumer software is something that there could be sales here in New York. There could be sales anywhere. But the marketing is not targeted toward anybody in New York.

This is a generally accessible website available to anybody in the world. If users in New York decide that they want to purchase the add-on for the premier version, they can do so just like anybody else in the country. There is no targeting toward New York. That is really what is the focus in several of the more recent cases addressing personal jurisdiction in the context of Internet sales.

THE COURT: Are you making right now a personal jurisdiction argument or the transfer argument or both?

MR. NEWBY: This particular argument has to do with personal jurisdiction. It shows the weakness of personal

jurisdiction in this case, which is why it is also appropriate to consider the transfer motion first. Plaintiffs have pointed to a handful, I think it was less than 10 percent, of their customers that they consider to have been affected by the update that Malwarebytes did who are located in New York. By that logic, 90 percent of their customers who are affected by this were located elsewhere. It shows the de minimis connection of this case to New York.

THE COURT: Plaintiffs also say that as to some of the witnesses they would call, they are located at least in or around the metropolitan area.

MR. NEWBY: That's correct. As we understood their declaration, most of their witnesses, employees, work in the Connecticut area. There is one who worked overseas. None is located in New York. But yes, your Honor, within 100 miles or less of New York.

THE COURT: Your submission I don't think goes witness by witness, does it?

MR. NEWBY: We don't identify specific witnesses by name. That is to say that every single witness who we would call --

THE COURT: Here is the problem. On these transfer motions the court is, at least in part, supposed to make a very tactile pragmatic assessment of what a trial looks like. It is for that reason that it used to be, when we had things called

documents, that the location of the documents took on weight. That is less so now in the electronic world. But it still matters as to the who, who is going to be inconvenienced, who is going to be testifying.

One naturally puts less weight on a broad-gauge assertion that all our witnesses are not New Yorkers. Usually one wants to get a sense of what does this trial look like, who are these witnesses, what are they going to be testifying to, who are central, who are exchangeable. It allows the Court to make that sort of an assessment. I was struck, having resolved a number of transfer motions over time, by the lack of an atomized concrete portrait, if you will, of trial witnesses.

MR. NEWBY: That is because, your Honor, there is a team of engineers and personnel who work at Malwarebytes in Santa Clara in California who would all be likely witnesses in this case, as well as Mr. Harris, who has already submitted a declaration as to the competition or lack thereof between the companies.

The main issue here is that we are not an organization that has witnesses spread all over the country. Every single one of the witnesses, the engineers involved in the creation of the PUP criteria and refinement of those criteria is based in Santa Clara. Those are the witnesses that we would call.

THE COURT: What about the witnesses from Enigma? Are you in a position to contest what Enigma is saying as to who

from its perspective would be called?

MR. NEWBY: The analysis that courts have looked at is what is the materiality and how significant are these witnesses to the claims in the case. The significance of plaintiff's claims is that we, Malwarebytes, created this update in bad faith and that our software works in such a way that it makes it difficult for consumers to understand and turn on the white list function to enable the Spyhunter software to work on their computers in harmony with Malwarebytes. None of that testimony is going to come from an Enigma witness.

THE COURT: At a minimum, though, Enigma witnesses would be relevant to damages, correct?

MR. NEWBY: Yes, absolutely, your Honor. We are not saying there are zero witnesses.

THE COURT: Some Enigma witness or witnesses would need to describe the impact of what Enigma's business model was and therefore help establish the fact and metes and bounds of the alleged violation of law even if you're right that the bulk of the witnesses would be inward-looking within Malwarebytes.

MR. NEWBY: I think that testimony and that witness would overlap completely with the damages. It would be what is the impact on Enigma. We are not taking the position that there are no witnesses who are based in the New York area who would be relevant, but the balance of witnesses. The most important witnesses on the liability issues are located in