UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

CASE NO. 20-60416-CIV-CANNON/Hunt

TOCMAIL INC,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.
_____/

ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

THIS CAUSE comes before the Court upon Plaintiff's Motion for Summary Judgment ("Plaintiff's Motion") [ECF No. 96] and Defendant's Motion for Summary Judgment ("Defendant's Motion") [ECF No. 98]. The Court has reviewed Plaintiff's Motion, Defendant's Motion, and the full record [ECF Nos. 95, 97, 100, 109, 110, 111, 112, 114, 115, 116, 117]. Upon careful review, Plaintiff's Motion for Summary Judgment is **DENIED**, and Defendant's Motion for Summary Judgment is **GRANTED**.

FACTUAL BACKGROUND[1]

This case involves alleged false or misleading advertising under the Lanham Act based on Microsoft's promotion of its cybersecurity software. The material facts viewed in the light most favorable to Plaintiff as the non-moving party are as follows.

[1] These facts are drawn from the parties' Joint Statement of Undisputed Facts [ECF No. 95], Plaintiff's Statement of Material Facts [ECF No. 97], Defendant's Statement of Material Facts [ECF No. 100], Plaintiff's Opposition Statement of Facts [ECF No. 110], Defendant's Opposition Statement of Facts [ECF No. 112], Plaintiff's Reply Statement or Facts [ECF No. 116], Defendant's Reply Statement of Facts [ECF No. 117], and supporting exhibits. Wherever there is a factual dispute, the Court construes the record in a light most favorable to Plaintiff.

Plaintiff TocMail Inc. ("TocMail") filed this suit against Microsoft Corporation ("Microsoft") seeking injunctive relief and damages for alleged violations of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), for false or misleading advertising of its link scanning service, Safe Links [ECF No. 42 ¶ 106]. Microsoft's allegedly deceptive ads are detailed further below. *See infra* pp. 4–5.

Safe Links is a cybersecurity feature within Microsoft's cloud-based email filtering service that was originally named "Advanced Threat Protection" ("ATP") and later renamed "Microsoft Defender for Office 365" ("Defender") [ECF No. 95]. Defender generally provides anti-phishing and anti-malware protection, among other things [ECF No. 100 ¶ 9; ECF No. 110 ¶ 9]. Microsoft introduced Safe Links in 2015, alongside another service called Safe Attachments, as a service that protects users from malicious URLs [ECF No. 95 ¶ 2; ECF No. 97 ¶ 1; ECF No. 100 ¶ 1]. The term URL refers to a link to a website within a document that takes users to a particular online web address [ECF No. 97 ¶ 3; ECF No. 112 ¶ 3]. Safe Links began as a reputation service that checks URLs against a list of known malicious links [ECF No. 97 ¶ 2; ECF No. 112 ¶ 2]. Microsoft later added another capability to Safe Links called URL detonation, which analyzes the web content linked to by the URL to "determine whether that website is good or bad" [ECF No. 97 ¶¶ 7–8; ECF No. 112 ¶¶ 7–8; ECF No. 97-15; ECF No. 97-6 pp. 5:3–20, 11:22–23]. Links that pass through the reputation check then go to the detonation service for analysis [ECF No. 97 ¶ 8; ECF No. 112 ¶ 8]. Microsoft internally refers to its detonation service as "Sonar" [ECF No. 97 ¶ 8; ECF No. 112 ¶ 8]. Together, reputation and detonation "are the two primary components" of Safe Links [ECF No. 97 ¶ 8; ECF No. 112 ¶ 8]. Microsoft internally refers to instances where its detonation check wrongly classifies a malicious link as benign as a "false negative" or "FN" [ECF No. 97 ¶ 9; ECF No. 112 ¶ 9].

Hackers use various forms of "evasion"—techniques that disguise malicious content and make it appear benign—to circumvent cybersecurity software [ECF No. 110-1 p. 7:3–8;

ECF No. 112 ¶ 6; ECF No. 116 ¶ 6]. Microsoft has identified several broad types of evasion, including sandbox evasion, app level evasion (or browser-based evasion), geo evasion, time delayed evasion (or time-based evasion), human based evasion, and IP evasion (also sometimes referred to as network evasion) [ECF No. 110-1 p. 7:13–22; ECF No. 97-20 pp. 3, 20; ECF No. 97-53 p. 2 ("Attackers are preventing our ability to see the phish content/landing pages due to various types of evasion techniques . . . .")]. IP evasion means that phishing URLs use the visitor's IP address to determine whether that visitor is a human user or security software and then display different content accordingly [ECF No. 97 ¶ 11 ("[O]ur definition of IP evasion[:] an attacker can create a link where when Sonar visits that link the attacker can determine the IP ranges of our visit. . . . [I]f they determine our visit from Sonar detonation is coming from Microsoft's IP range they can choose to use that information to display whatever web page they wish to."); ECF No. 112 ¶ 11]. Attackers then send benign content to the security scanner and malicious content to the intended victims [ECF No. 97 ¶ 11; ECF No. 112 ¶ 11]. IP evasion is "a common tactic" that attackers use today [ECF No. 97 ¶ 12; ECF No. 112 ¶ 12]. TocMail uses the term "IP cloaking" for what Microsoft calls IP evasion; those terms are interchangeable [ECF No. 97 ¶ 11; ECF No. 112 ¶ 11].

Microsoft staff were aware of the existence of IP evasion in 2016 and even as early as 2010 [ECF No. 97 ¶ 15; ECF No. 112 ¶ 15]. Safe Links is not 100% effective against malicious URLs using IP evasion [ECF No. 100 ¶ 6]. A slide from a March 2017 internal Microsoft titled "Why does detonation have false negatives?" identified IP evasion as an issue [ECF No. 97-37 p. 42 ("Sonar currently does not use un-attributable network space for routing detonation network traffic. . . . Attackers can easily attribute the traffic to Microsoft and not serve the phish content")]. Microsoft recognized that IP evasion was a problem for Safe Links, particularly around 2018 as phishing attacks using IP evasion "started escalating" [ECF No. 97-6 p. 17:21–25]. For example, an internal Microsoft email sent on June 28, 2018 describes a recent incident where Safe Links did

not detect a malicious URL sent to a client's CEO that used "IP based evasion" [ECF No. 97-41 p. 3]. The email adds that "[t]his was also called out by the Sonar Analyst team as one of the top reasons for [false negatives]," and that "in the case of a targeted attack[,] it is easy for an attacker to only display malicious content in specific targeted IP ranges" [ECF No. 97-41 p. 3]. In November 2018, Microsoft launched a new feature within Safe Links called IP Anonymization [ECF No. 97 ¶ 28; ECF No. 112 ¶ 12]. IP Anonymization was intended to help counteract IP evasion by routing detonation web traffic through third-party IP addresses [ECF No. 100 ¶ 5]. IP evasion is a topic that sometimes came up between Microsoft and customers, with at least one customer asking "[w]hy is an IP-address range used which is easily attributable to Microsoft?" [ECF No. 97-90 p. 5]. According to Microsoft's internal "talking points" for a meeting with that customer, Microsoft's response included discussion of IP Anonymization as a partial solution within Microsoft's "layered defense" approach to evasion [ECF No. 97-90 pp. 5, 8–9].

In December 2019, TocMail's namesake product, "TocMail"—a cloud-based, email security service that competes with Safe Links—became available for purchase [ECF No. 95 ¶ 4; ECF No. 97 ¶ 43; ECF No. 95-5, p. 5].

Microsoft's Promotion of Safe Links

Microsoft promoted its Safe Links service through various brochures, product guides, and other promotional materials [ECF No. 97 ¶¶ 44–51; ECF No. 100 ¶ 14]. At issue in this case are three messages promoting Safe Links [ECF No. 42 ¶¶ 56–75].

Message #1

The first message promoting Safe Links, which appears in both video and print, states:

> Sophisticated attackers will plan to ensure links pass through the first round of security filters. They do this by making the links benign, only to weaponize them after the message is delivered, altering the destination of the links to a malicious

> site. . . . With Safe Links, we are able to protect users right at the point of click by checking the link for reputation and triggering detonation if necessary.

[ECF No 97-63; ECF No. 97-64; ECF No. 97-66 p. 9].

Message #2

The second message promoting Safe Links, which appears on Microsoft's website, blog, and ATP Product guide, provides:

> EOP scans each message in transit in Office 365 and provides time of delivery protection, blocking any malicious hyperlinks in a message. But attackers sometimes try to hide malicious URLs within seemingly safe links that are redirected to unsafe sites by a forwarding service after the message has been received. The ATP Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, so malicious links are dynamically blocked while good links can be accessed.

[ECF No. 97-1 p. 2; ECF No. 97-36 p. 6; ECF No. 97-70 p. 3].

Message #3

The third message promoting Safe Links, which appears in a promotional slide presentation and Pitch Deck, states: "[e]nsure users are protected against URLs that redirect to malicious sites. Safe Links will proactively protect your users every time they click a link, ensuring malicious links are dynamically blocked even if they are changed after the message has been received" [ECF No. 97-30 p. 15; ECF No. 97-71 p. 20 ("Ensure hyperlinks in documents are harmless with ATP Safe Links")].

PROCEDURAL HISTORY

TocMail filed its complaint on January 10, 2020 [ECF No. 1]. The initial complaint raised two counts arising under 15 U.S.C. § 1125(a)(1)(B) of the Lanham Act: False Advertising (Count One) and Contributory False Advertising (Count Two) [ECF No. 1 ¶¶ 189, 205]. Microsoft then moved to dismiss both counts on the basis that TocMail lacked standing and failed to state a claim for which relief could be granted [ECF No. 14]. The Court denied the motion as to Count One and dismissed Count Two, giving TocMail leave to file an Amended Complaint [ECF No. 41].

TocMail then filed the operative First Amended Complaint, which contains a single count for False and Misleading Advertising under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B) [ECF No. 2 ¶ 106]. TocMail seeks monetary damages as well as temporary and permanent injunctive relief enjoining Microsoft from continuing to promote its Safe Links service using the same allegedly deceptive messages [ECF No. 42 p. 29–30]. Microsoft moved unsuccessfully to dismiss the single count in the First Amended Complaint for failure to state a claim [ECF No. 44; ECF No. 104].

On July 9, 2021, TocMail and Microsoft each filed opposing Motions for Summary Judgment [ECF Nos. 96, 98]. The Motions are ripe for adjudication [ECF Nos. 109, 111, 114, 115].

LEGAL STANDARD

Summary judgment is appropriate where there is "no genuine issue as to any material fact [such] that the moving party is entitled to judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); Fed R. Civ. P. 56(a). An issue of fact is "material" if it might affect the outcome of the case under the governing law. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). It is "genuine" if the evidence could lead a reasonable jury to find for the non-moving party. *See id.*; *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

At summary judgment, the moving party has the burden of proving the absence of a genuine issue of material fact, and all factual inferences are drawn in favor of the non-moving party. *See Allen v. Tyson Foods Inc.*, 121 F.3d 642, 646 (11th Cir. 1997). The Court, in ruling on a motion for summary judgment, "need consider only the cited materials, but it may consider other materials in the record." Fed. R. Civ. P. 56(c)(3). The non-moving party's presentation of a "mere existence of a scintilla of evidence" in support of its position is insufficient to overcome summary judgment. *Anderson*, 477 U.S. at 252.

"For factual issues to be considered genuine, they must have a real basis in the record." *Mann v. Taser Int'l, Inc.*, 588 F.3d 1291, 1303 (11th Cir. 2009) (internal quotation marks omitted). Speculation or conjecture cannot create a genuine issue of material fact. *Cordoba v. Dillard's, Inc.*, 419 F.3d 1169, 1181 (11th Cir. 2005). The moving party has the initial burden of showing the absence of a genuine issue as to any material fact. *Clark v. Coats & Clark, Inc.*, 929 F.2d 604, 608 (11th Cir. 1991). In assessing whether the moving party has met this burden, the court must view the movant's evidence and all factual inferences arising from it in the light most favorable to the non-moving party. *Denney v. City of Albany*, 247 F.3d 1172, 1181 (11th Cir. 2001). Once the moving party satisfies its initial burden, the burden shifts to the non-moving party to come forward with evidence showing a genuine issue of material fact that precludes summary judgment. *Bailey v. Allgas, Inc.*, 284 F.3d 1237, 1243 (11th Cir. 2002); Fed. R. Civ. P. 56(e).

DISCUSSION

Microsoft asserts that it is entitled to summary judgment on the false advertising claim because the allegedly deceptive ads promoting Safe Links were neither "false" nor "misleading" within the meaning of 15 U.S.C. § 1125(a)(1) [ECF No. 98 pp. 13–25]. Microsoft also argues that summary judgment is warranted in its favor because (1) TocMail has not met its burden to show that the ads were material to consumers' purchasing decisions [ECF No. 98 pp. 25–28]; and (2) TocMail has failed to show that it has been or likely will be injured as a result of the allegedly deceptive ads [ECF No. 98 pp. 28–34].

The Lanham Act provides a civil cause of action for false advertising as set forth below:

> (1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
>
> (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

> (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,
>
> shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a).

To state a claim under 15 U.S.C. § 1125(a), a plaintiff must establish the following elements:

> (1) the ads of the opposing party were false or misleading, (2) the ads deceived, or had the capacity to deceive, consumers, (3) the deception had a material effect on purchasing decisions, (4) the misrepresented product or service affects interstate commerce, and (5) the movant has been—or is likely to be—injured as a result of the false advertising.

Johnson & Johnson Vision Care, Inc. v. 1-800 Contacts, Inc., 299 F.3d 1242, 1247 (11th Cir. 2002). If an advertisement is deemed "to be literally false, the [plaintiff] need not present evidence of consumer deception." *Id.* If an advertisement is deemed "to be true but misleading, the [plaintiff] . . . must present evidence of deception." *Id.*

In this case, TocMail asserts that the allegedly deceptive ads are literally false rather than merely misleading, and therefore, TocMail need not present evidence of deception to meet its burden on the first element [ECF No. 96 p. 23]. Thus, the threshold issue in this case is whether the Microsoft ads at issue are literally false under 15 U.S.C. § 1125(a)(1).

Literal Falsity

The false or misleading element is satisfied if "the challenged advertisement is literally false, or if the challenged advertisement is literally true, but misleading." *Johnson & Johnson Vision Care, Inc. v. 1-800 Contacts, Inc.*, 299 F.3d 1242, 1247 (11th Cir. 2002). "When determining whether an advertisement is literally false or misleading, courts 'must analyze the message conveyed in full context,' and 'must view the face of the statement in its entirety.'"

Osmose, Inc. v. Viance, LLC, 612 F.3d 1298, 1308 (11th Cir. 2010) (quoting *1-800 Contacts, Inc.*, 299 F.3d at 1248)). On the other hand, mere "puffery" is not actionable under the Lanham Act and generally comes in one of two possible forms: "(1) an exaggerated, blustering, and boasting statement upon which no reasonable buyer would be justified in relying; or (2) a general claim of superiority over comparable products that is so vague that it can be understood as nothing more than a mere expression of opinion." *Pizza Hut, Inc. v. Papa John's Intern., Inc.*, 227 F.3d 489, 496–97 (5th Cir. 2000).

"The distinction between literally false and merely misleading statements is often a fine line." *Osmose, Inc.*, 612 F.3d at 1308. "The ambiguity of the statement at issue, or the lack thereof, is significant." *Id.* "Statements that have an unambiguous meaning, either facially or considered in context, may be classified as literally false." *Id.* at 1309 (citing *United Indus. Corp. v. Clorox Co.*, 140 F.3d 1175, 1180 (8th Cir. 1996)); *Time Warner Cable, Inc. v. DIRECTV, Inc.*, 497 F.3d 144, 158 (2d Cir. 2007) ("[O]nly an unambiguous message can be literally false."). "The greater the degree to which a message relies upon the viewer or consumer to integrate its components and draw the apparent conclusion, however, the less likely it is that a finding of literal falsity will be supported." *United Industries Corp. v. Clorox Co.*, 140 F.3d 1175, 1181 (8th Cir. 1998). "Commercial claims that are implicit, attenuated, or merely suggestive usually cannot fairly be characterized as literally false." *Id.*

TocMail argues that the ads at issue are literally false because they necessarily imply a falsehood: that Safe Links "provides effective protection" against URLs that use IP evasion [ECF No. 96 p. 22]. That implied message is false, TocMail contends, because Safe Links does not sufficiently protect against redirected links using IP evasion to avoid detonation [ECF No. 96 p. 22]. In support, TocMail points to evidence in the record, including Microsoft's internal communications, highlighting "gaps" in protection based on IP Evasion that could be "easily" bypassed [ECF No. 97-53 p. 2; ECF No. 97-20 p. 15].

Microsoft argues that the ads are not literally false because they do not advertise Safe Links as the "solution" to IP evasion or even say anything about IP evasion [ECF No. 98 pp. 14–15]. Rather, Microsoft argues that Safe Links works as advertised by deploying its reputation and detonation services to detect malicious links [ECF No. 98 pp. 15–19]. Microsoft points out that it does not guarantee that Safe Links will block every single type of attack every single time, adding that Microsoft has at various times, including in public facing Q&A documents, disclaimed that it provides this sort of infallible protection [ECF No. 98 p. 21; ECF No. 100-13 p. 3]. Microsoft further argues that the language in Message #3—"[e]nsure document hyperlinks are harmless with ATP Safe Links"—is non-actionable puffery, and that in any event, Message #3 is not deceptive when read in context [ECF No. 98 pp. 20–21]. Finally, Microsoft argues that the ads are not even misleading because their intended audience is technologically sophisticated and would not interpret the ads as promising impervious protection [ECF No. 98 pp. 22–23].

Upon review of all of the ads in their full context, the Court finds that the allegedly deceptive messages are not literally false because they are ambiguous. Claims for literal falsity must fail if "the statement can reasonably be understood as conveying different messages." *Zoller Laboratories, LLC. v. NBTY, Inc.*, 111 F. App'x 978, 983 (10th Cir. 2004) (citing *Scotts Co. v. United Industries Corp.*, 315 F.3d 264, 275 (4th Cir. 2002) ("Because the graphic can reasonably be understood as conveying different messages, Scotts' literal falsity argument must fail."); *see also Time Warner Cable, Inc. v. DIRECTV, Inc.*, 497 F.3d 144, 158 (2d Cir. 2007) ("[I]f the language or graphsic is susceptible to more than one reasonable interpretation, the advertisement cannot be literally false.").

In this case, each of the ads at issue reasonably could be interpreted in multiple ways. One possible interpretation, for example, is that the ads describe at a basic level *what* Safe Links does—it blocks malicious links by deploying both its reputation and detonation components. This occurs at the time a user clicks on the link rather than when the message is sent. In other words, every

time a user clicks on a link it triggers both components of Safe Links. Microsoft employee Amar Patel explains this interpretation, discussing Message #2 as follows:

> And this statement is indicating that . . . Safe Links protection service will have the opportunity to evaluate that link with two measures. The first will be the reputation service, the second will be time-of-click detonation, and that's what this is saying. So, you know, from my standpoint both points are true. The first point being we don't offer 100 percent protection and the second point being that if Safe Links is turned on for a given user that user has the opportunity to be protected by Safe Links by virtue of that click being routed to the Safe Links protection service and being evaluated by, again, reputation and detonation.

[ECF No. 100-6 pp. 15:12–16:3].

This interpretation is reasonable in the context of the ads because other statements in those ads undercut the impression that Microsoft is promoting 100% protection. For example, the ads state that Safe Links "**mitigate[s]** malicious content" and "**helps** prevent users from going to malicious websites when they click them in email" [ECF No. 97-66 p. 12; ECF No. 97-36 p. 9 (emphasis added)]. The ads also contain statements suggesting that Safe Links' protection is variable depending on a user's settings [ECF No. 97-71 p. 20 ("Protect your organization from harmful hyperlinks through ATP **Safe Links policies**. Create a custom blocked URL list for **more advanced** protection") (emphasis added)]. In one case, an ad explicitly states that Microsoft does not guarantee 100% protection [ECF No. 97-72 p. 11 ("No solution is 100% effective, and that makes it important to have an 'assume breach' mindset.")].

Still, TocMail contends that the ads at issue unambiguously promise "effective protection" [ECF No. 96 p. 22]. In particular, TocMail argues that the language in Message #3 (that Safe Links "ensure[s] hyperlinks in documents are harmless") "does promote Safe Links as providing guaranteed (i.e. 100%) safety" based on a dictionary definition of the word "ensure" as synonymous with "guarantee" [ECF No. 110 ¶ 20]. While the Court agrees with TocMail that its

interpretation is one possible interpretation,[2] TocMail's reading omits the full context of the ads and is therefore insufficient to demonstrate literal falsity. *See Schering-Plough Healthcare Products, Inc. v. Schwarz Pharma, Inc.*, 586 F.3d 500, 513 (7th Cir. 2009) (Posner, J.) ("A 'literal' falsehood is bald-faced, egregious, undeniable, over the top. . . . The proper domain of 'literal falsity' as a doctrine that dispenses with proof that anyone was misled or likely to be misled is the patently false statement that means what it says to any linguistically competent person . . . .") (citing *Avis Rent A Car System, Inc. v. Hertz Corp.*, 782 F.2d 381, 385 (2d Cir. 1986) (Friendly, J.) ("Fundamental to any task of interpretation is the principle that text must yield to context.")).

Relevant here is the fact that Microsoft is promoting a cybersecurity service to business enterprise customers, with the intended audience consisting of IT professionals well-versed in the cybersecurity industry [ECF No. 100-12 p. 8:10–12]. Fundamental to the cybersecurity industry is the reality that security threats are "constantly evolving" [ECF No. 100 ¶ 12; ECF No. 100-6 p. 12:16–19 ("We work in the security industry, our adversaries are software professional hackers and they are trying to dream up new ways to counteract or circumvent the security measures that we provide."); ECF No. 110-12 pp. 6:13–14, 10:11–15 ("[T]his is software. Nothing is always 100 percent. . . . [O]bviously new attacks are coming all the time.")]. Because of this dynamic threat landscape, Microsoft explicitly disclaims—in public facing documents such as Office 365 ATP FAQs and even in one of the allegedly deceptive ads TocMail raises—that its software does not catch 100% of malicious attacks [ECF No. 100-13 p. 3 ("Will ATP catch 100% of malicious attacks? No. In fact, no advanced threat protection product can catch 100% of malicious attacks, despite claims to the contrary."); ECF No. 97-72 p. 11].

[2] Although Message #3 is vague and generalized, the Court does not find that the word "ensure" is non-actionable puffery since it is neither a statement of superiority nor quite so exaggerated that no reasonable consumer would be justified in relying upon it. *See Pizza Hut, Inc. v. Papa John's Intern., Inc.*, 227 F.3d 489, 496–97 (5th Cir. 2000). The record demonstrates that at least some Microsoft customers have the "common misapprehension" that "no phishing emails . . . should reach users" [ECF No. 110-12 p. 3].

In light of this context, the Court finds that this sophisticated audience reasonably could interpret Message #3 as not promising 100% protection against every threat. *See Buetow v. A.L.S. Enterprises, Inc.*, 650 F.3d 1178, 1186 (8th Cir. 2011) (reversing the district court's literal falsity finding that relied on a dictionary definition and finding that the term "odor eliminating" as stated in an ad for hunting clothes was not literally false, because the court "doubt[ed] there are many hunters so scientifically unsophisticated as to believe that any product can 'eliminate' every molecule of human odor"); *see also SmithKline Beecham Consumer Healthcare, L.P. v. Johnson & Johnson-Merck Consumer Pharm. Co.*, No. 01 CIV. 2775, 2001 WL 588846, at *9 (S.D.N.Y. June 1, 2001), *aff'd*, 19 F. App'x 17 (2d Cir. 2001) ("[C]ourts should use logic and common sense to determine the literal meaning of an advertisement. Moreover, relevant to any such determination is both the intended audience of the commercial and the intended product usage."). In sum, because the ads at issue are susceptible to multiple reasonable interpretations when read in context, TocMail has failed to demonstrate that they are literally false.

Actual Deception

Even if not literally false, the advertisements still may be actionable under § 1125(a)(1) if they are "misleading." 15 U.S.C. § 1125(a)(1). To show that an advertisement is "misleading, the [plaintiff] . . . must present evidence of deception." *Johnson & Johnson Vision Care, Inc. v. 1-800 Contacts, Inc.*, 299 F.3d 1242, 1247 (11th Cir. 2002). "While 'full-blown consumer surveys or market research are not an absolute prerequisite,' the moving party must provide 'expert testimony or other evidence." *Id.* (quoting *United Industries Corp. v. Clorox Co.*, 140 F.3d 1175, 1183 (8th Cir. 1998)). "Plaintiff cannot obtain relief simply by arguing how consumers could react, rather, it must show how consumers actually react." *BellSouth Advert. & Pub. Corp. v. Lambert Pub.*, 45 F. Supp. 2d 1316, 1321 (S.D. Ala. 1999), *aff'd sub nom. BellSouth Adv. v. Lambert Pub.*, 207 F.3d 663 (11th Cir. 2000).

In this case, there is no dispute that TocMail did not conduct any consumer survey or poll demonstrating consumer deception [ECF No. 100 ¶ 40; ECF No. 110 ¶ 40]. Nor did TocMail engage any expert to conduct causation analysis as to whether the ads actually deceived consumers; TocMail's damages expert testified that her analysis *assumed* consumers were deceived by the ads [ECF No. 100 ¶ 41; ECF No. 110 ¶ 41]. More to the point, TocMail's Motion does not address actual deception at all, relying solely on literal falsity and affirmatively eschewing the need to proffer evidence of deception [ECF No. 96 p. 23; ECF No. 114 p. 10]. Nevertheless, out of an abundance of caution, the Court notes that TocMail presents the following in one of its statements of material facts as evidence of consumer deception: Microsoft's internal emails and documents discussing a question, submitted by a customer on May 19, 2020, that raises IP evasion as a possible security concern [ECF No. 110 ¶ 40; ECF No. 97-90 p. 5]. Specifically, Microsoft's internal document, titled "BOSCH DISCUSSION PREP," includes the following prepared talking point in response to a customer asking "[w]hy is an IP-address range used which is easily attributable to Microsoft?":

> We selectively route detonations through an IP anonymization network. All detonations are not routed out Microsoft IP ranges. We monitor network evasion on a weekly basis and corelate signals with our endpoint security services and TI to ensure effectiveness. We're also exploring new ideas such as collaborating with customers to route detonations for their tenant out their IP ranges via VPN.

[ECF No. 97-18 p. 4]. This evidence—which consists of a Microsoft customer apparently asking about Safe Links' vulnerability to IP evasion, followed by Microsoft's emphasis in a talking point of its IP anonymization feature and other services/ideas to protect against IP evasion—does not show any customer reaction or otherwise show the customer was deceived into thinking that Microsoft's product provides foolproof protection against IP evasion. Nor does TocMail offer anything else to substantiate actual deception. *See Miller's Ale H., Inc. v. Boynton Carolina Ale H., LLC*, 745 F. Supp. 2d 1359, 1377 (S.D. Fla. 2010), *aff'd*, 702 F.3d 1312 (11th Cir. 2012)

(finding no actual deception where plaintiff did not adduce any reliable consumer or market research showing deception and instead produced only anecdotal evidence).

For these reasons, TocMail has not met its burden to show that the subject messages disseminated by Microsoft are either literally false or misleading within the meaning of the Lanham Act, under 15 U.S.C. § 1125(a)(1).[3] Summary judgment in favor of Microsoft is warranted.

CONCLUSION

For the foregoing reasons, it is **ORDERED AND ADJUDGED** as follows:

1. Defendant's Motion for Summary Judgment [ECF No. 98] is **GRANTED**. Summary judgment is hereby **ENTERED** in favor of the Defendant.
2. The Court will enter a separate final judgment pursuant to Federal Rule of Civil Procedure 58.

DONE AND ORDERED in Chambers at Fort Pierce, Florida this 21st day of December 2021.

AILEEN M. CANNON
UNITED STATES DISTRICT JUDGE

cc: counsel of record

[3] The Court need not address Defendant's other arguments based on materiality or injury [ECF No. 98 pp. 25–28, 28–34].