UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Civil Action No.:

TOCMAIL INC, a Florida corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.
_____/

COMPLAINT

Plaintiff, TOCMAIL INC ("Plaintiff" or "TocMail"), by and through undersigned counsel, sues Defendant, MICROSOFT CORPORATION ("Defendant" or "Microsoft"), and alleges as follows:

NATURE OF ACTION

1. This is an action for damages in excess of $43 billion, injunctive relief, and disgorgement of profits under the Lanham Act for harm suffered by Plaintiff and from future harm Plaintiff will suffer due to Microsoft's dissemination of deceptive promotions of its Safe Links service.

2. Plaintiff's CEO, who previously sold a prior internet invention for stock from MicroMuse (which value exceeded $95 million when the stock lockup period expired), currently offers a patented solution to the most common, most effective cloud-based hacking attack. However, Plaintiff is hindered from selling its patented solution because Microsoft falsely claims to have solved this same issue four years ago.

3. Prior to Plaintiff's patent, cloud security had a flaw that allowed hackers to evade cloud-based scanners virtually 100% of the time. Companies avoided migrating to the cloud because they were duly warned about cloud security's Achilles heel. Without fixing the flaw, Microsoft convinced companies that they could safely move to the cloud, promising its Safe Links service will protect them from cloud security's Achilles heel. However, Microsoft knew that Safe Links did not offer any such protection. In order to procure billions in annual income, Microsoft knowingly made these companies *defenseless* against the very attack it promised protection from. Approximately 100 million professionals currently subscribe to Microsoft's Safe Links service for the express purpose of being protected against the most common, most effective cloud-based attack. Meanwhile, all of them can now be effortlessly (and secretly) hacked at will.

4. From a technical perspective, Safe Links is a time-of-click redirection service (i.e., it attempts to redirect users to either a warning page or to a safe site each time the user clicks a link). Therefore, 100 million professionals have expressed their desire to subscribe to a time-of-click redirection service that thwarts the most common, most effective cloud-based attack. Plaintiff holds a patent on the only time-of-click redirection service designed to block this attack. Because all 100 million professionals believe that they are already receiving this service from Microsoft, they wrongly perceive Plaintiff's solution as offering no value to them.

5. Given that no professional would willingly make themselves defenseless against the very attack they are purchasing protection from, the number of customers that Microsoft diverts away from Plaintiff does not require any speculation. Even should Microsoft cease its false advertising, harm to Plaintiff would continue due to Microsoft's retention of customers that it has already deceived. Given that Plaintiff holds a patent on the only time-of-click redirection service immune to this attack, the duration of the continued damage also does not require speculation (the

duration lasting until the patent's expiration on May 7, 2035). Plaintiff loses $2.50 per month per user diverted to Microsoft due to Microsoft's false advertising. This results in $43 billion in damages over the lifetime of the patent. Plaintiff is seeking monetary relief for the full amount of the damages.

6. Microsoft knowingly and intentionally engages in false advertising. In 2017, a security researcher notified Microsoft in writing of Safe Links' inability to stop the very attack that Microsoft promises Safe Links protects against. The email exchange between Microsoft and this researcher documents that Microsoft has full knowledge of Safe Links' inability to protect against this specific attack. The email exchange further documents that Microsoft does not expect Safe Links to ever be able to protect against this attack, acknowledging that *Safe Links was never designed to do so*. Nevertheless, Microsoft continues to convince companies to move to their cloud by promising Safe Links will protect them against the same attack that it secretly acknowledges Safe Links is unable to protect against. Plaintiff is seeking disgorgement of profits. There is great public interest in making this misconduct unprofitable. Plaintiff is seeking three times Defendant's profits made as a result of Defendant's wrongful actions or three times Plaintiff's damages, whichever is greater.

7. Microsoft has also irreparably harmed Plaintiff's reputation and continues to irreparably harm Plaintiff's reputation, by convincing over 100 million professionals that Plaintiff's offering is of no value to them, even though these professionals can be hacked at will and therefore need Plaintiff's cybersecurity service. Plaintiff is seeking injunctive relief.

8. Microsoft also engages in contributory false advertising, playing a significant role in convincing approximately 1 billion consumers to wrongly believe that the fundamental cloud security weakness was fully solved many years ago. Microsoft, Symantec, Mimecast, ProofPoint,

Sophos, Barracuda, and Vade Secure all openly acknowledge that the cloud security flaw still allows emails with a certain type of malicious link to be delivered to inboxes virtually 100% of the time, regardless of the cloud-based security being used (regardless of blacklists, regardless of artificial intelligence, regardless of machine learning, etc.). All of these companies specifically promote their time-of-click redirection services as effective solutions to the problem, even though all of them contain the exact same design flaw that literally renders them *defenseless*. Microsoft benefits greatly when professionals subscribe to their cloud-based apps (such as Office 365) even when professionals choose a third-party for protection. Microsoft provides various cybersecurity vendors with access to its users' email and data via proprietary protocols. It provides other forms of technology and assistance to other cybersecurity vendors in order to further the perception that it is safe for companies to move to Microsoft's cloud. Consumers en masse have been irrevocably deceived through the reinforcement of false messaging from a myriad of highly trusted security vendors, much to the benefit of Microsoft who significantly enables it.

THE PARTIES

9. Plaintiff, TocMail, is a Florida corporation doing business within this District.

10. Defendant, Microsoft, is a Washington corporation with, upon information and belief, its principal place of business in Redmond, Washington doing business throughout the United States, including within this District. Microsoft is registered to do business in the State of Florida, and has one of its corporate headquarters located within this District as well.

JURISDICTION AND VENUE

11. This is a civil action for damages in excess of $43 billion, disgorgement of profits and injunctive relief for, among other things, false and misleading advertising under 15 U.S.C. §

1125(a)(1)(B). Plaintiff is seeking judgement for three times profits or damages, whichever is greater, pursuant to 15 U.S.C. § 1117(a).

12. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because TocMail's claims arise under federal law, as well as pursuant to 15 U.S.C. § 1121 because TocMail's claims arise under the Lanham Act.

13. This Court has personal jurisdiction over Microsoft because it is registered to do business in Florida, operates, conducts, engages in and carries on a business in Florida, including within this judicial district, has offices in Florida, and committed a tortious act within Florida, including within this judicial district. Thus, this Court's exercise of personal jurisdiction over Microsoft is consistent with the Constitution of the United States and Fla. Stat. § 48.193.

14. Venue is proper in the United States District Court for the Southern District of Florida pursuant to at least 28 U.S.C. §§ 1391.

GENERAL ALLEGATIONS

A. TocMail's Security Services.

15. Plaintiff's CEO is a software developer with expertise in modern high-level scripting languages, traditional low-level languages, and chip level programming via assembler. He previously invented, and served as the lead programmer of, data communication technology that was sold to MicroMuse for stock, the value of which exceeded $95 million when the stock lockup period expired. He has an established background in creating commercially reliable code for mission critical operations.

16. In regards to cybersecurity, Plaintiff's CEO is credited with inventing one of the strongest block ciphers in history. His cybersecurity invention is studied in the text book *Advanced*

Cryptography by Bruce Schneier. Plaintiff's CEO is also a published cybersecurity expert, and he has been awarded eight cybersecurity patents to date.

17. As will be discussed in more detail below, Plaintiff's CEO has now solved one of the biggest problems in cloud-based security that previously allowed hackers to implement an attack that was virtually 100% effective. Plaintiff sells cloud-based security with the solution to such attacks. However, Microsoft falsely claims that its Safe Links service also defeats this specific attack and has done so for years knowing that such is not the case.

B. Inherent Design Weakness in Cloud-Based Security.

18. Cloud security has a major flaw that is not present with onsite security. With onsite security, the scanner and the user's device share the same Internet address (since both devices access the Internet through the same gateway). However, with cloud security, the scanner has a different Internet address than the user's device, allowing hackers to know when their links are being accessed by the security scanner or by a user's device. Hackers simply deliver benign content when the scanner's Internet address connects, and deliver malicious content to everyone else. The scanner approves the link because it only encounters benign content, then the user is harmed by malicious content that the scanner never even knows about. This simple attack is virtually 100% effective against cloud scanners.

19. When cloaking malicious content is based on Internet addresses (IP addresses), the attack is sometimes referred to as IP cloaking. As early as 2011, IP cloaking was known to be "the most simple and effective approach." It was known to be "the most effective form of evasion, since it thwarts any sort of detection" by cloud-based security scanners:

> …to evade detection, a simple yet powerful approach is to cloak against scanners by serving malicious content to users but benign content to the detector. While there are many forms of cloaking, in this paper we focus on arguably **the most simple**

> **and effective approach: cloaking at the IP level**. To do so, malicious servers simply refuse to return malicious content to requests from certain IP addresses. . . .
>
> **IP Cloaking can be the most effective form of evasion, since it thwarts any sort of detection** by client honeypots or AV engines. For an adversary, IP-based cloaking is simple to deploy and usually requires only small changes to the web server's configuration… At the time of this writing, IP cloaking contributes significantly to the overall number of malicious web sites found by our system. (emphasis added)

See "Trends in Circumventing Web-Malware Detection," by Moheeb Abu Rajab, Lucas Ballard, Nav Jagpal, Panayiotis Mavrommatis, Daisuke Nojiri, Niels Provos, Ludwig Schmidt, July, 2011 (excerpt), a true and correct copy of which is attached hereto as **Exhibit "1."**

20. With IP cloaking, the type of security running on cloud servers does not matter. IP cloaking renders all security useless because that security only sees good content. IP cloaking renders artificial intelligence, machine learning, and even blacklists useless by making malicious content invisible to it all.

21. Prior to Microsoft's false advertising, companies generally knew to keep their scanning onsite to avoid becoming defenseless against this effective security bypass.

22. Knowledge of IP Cloaking hindered cloud adoption. As will be discussed, Microsoft falsely claimed to have solved this problem in order to convince companies to move their email security to Microsoft's cloud. Meanwhile, Microsoft knowingly makes these companies defenseless against the very attack it promises protection from. Currently, upon information and belief, approximately 100 million professionals trust Microsoft's promise to protect against this specific attack.

C. Microsoft's Advanced Threat Protection and Safe Links.

1. Description Of Advanced Threat Protection and Safe Links.

23. IP Cloaked links are dynamic (i.e. they deliver different content to different devices). They are the most commonly used form of malicious dynamic links.

24. Microsoft markets, advertises, promotes and sells a cloud-based cybersecurity service called Safe Links ("Safe Links"). Microsoft promotes Safe Links as a solution to malicious dynamic links. Microsoft offers Safe Links within its Advanced Threat Protection ("ATP") service, which operates inside Microsoft's cloud-based Exchange Online Protection ("EOP") servers.

25. Over a four year period, Microsoft engaged in a sustained marketing campaign to falsely promote the narrative that Safe Links solves the cloud security flaw of IP Cloaked links and, therefore, companies can safely move to Microsoft's cloud service. Various examples of Microsoft's deceptive marketing and promotional materials regarding Safe Links are attached as exhibits to this Complaint, including: (a) topmost portion of Microsoft's current website regarding ATP and Safe Links, attached hereto as **Exhibit "2"**; (b) a 2015 Exchange Online Advanced Threat Protection Product Guide, attached hereto as **Exhibit "3"**; (c) an excerpt from Microsoft's 2016 ATP Product Guide, attached hereto as **Exhibit "4"**; (d) an excerpt from Microsoft's Office 365 ProPlus Pitch Deck attached hereto as **Exhibit "5"** and an excerpt from Microsoft's Office 365 ProPlus Mac Pitch Deck, attached hereto as **Exhibit "6"**; (e) an excerpt from Microsoft's current ATP Product Brochure, attached hereto as **Exhibit "7"**; (f) an excerpt from a transcript of Microsoft's 2019 ATP Product Video, the transcript which is produced and distributed by Microsoft, attached hereto as **Exhibit "8"**; (g) excerpt from a 2019 case study regarding ATP, attached hereto as **Exhibit "9"**; (h) an excerpt from a 2019 Enterprise-Class Technology Webpage, attached hereto as **Exhibit "10"**; (i) an excerpt from a 2019 Optimal Security with Minimal Complexity Webpage, attached hereto as **Exhibit "11"**; (j) 2017 Office 365: Everything You

Wanted to Know, attached hereto as **Exhibit "12"**; (k) an excerpt from an ATP Partner Datasheet, attached hereto as **Exhibit "13"**; and (l) a 2019 Microsoft "Exchange Online Business Class Email System" brochure, attached hereto as **Exhibit "14."**

2. Microsoft's Deceptive Message #1: Safe Links Thwarts Malicious Dynamic Links.

26. In a transcript of a 2019 ATP Product Video produced by Microsoft, Microsoft states:

> So let me break this down by starting with the core of all prevention: detection. Now, we invest at least a billion dollars in this area annually. . . . Sophisticated attackers will plan to **ensure links pass through the first round of security filters by making the links benign, only to weaponize them once the message is delivered. Meaning that the destination of that link is altered later to point to a malicious site.** Time is important when **thwarting this type of attack**. 20% of all clicks happen within just five minutes of when an email is received, and with Safe Links, **we're able to protect users right at the point of click** by checking the link for reputation and triggering detonation if necessary.

See **Ex. 8** (emphasis added).

27. Microsoft is correct that dynamic links bypass Microsoft's first round of security, the same round of security that Microsoft claims to invest a billion dollars in annually.

28. However, it is literally false that Safe Links protects users by "thwarting this type of attack." Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

29. Statements that have an unambiguous meaning, either facially or considered in context, may be classified as literally false.

30. Microsoft asserts that an unambiguous service (Safe Links) protects consumers by "thwarting" an unambiguous "type of attack" ("links [that] pass through the first round of security filters by making the links benign, only to weaponize them once the message is delivered. Meaning that the destination of that link is altered later to point to a malicious site").

31. Microsoft unambiguously states that Safe Links protects users by thwarting the malicious use of dynamic links.

32. However, it is undisputed that Microsoft knows that Safe Links is *defenseless* against the most common form of malicious dynamic links (IP Cloaked links). For example, on January 14, 2017, Mikail Tunç ("Tunc") notified Microsoft's Security Response Center (MSRC) that hackers can use IP Cloaked links to bypass Safe Links in its entirety. A true and correct copy of an email chain between Tunc and MSRC is attached hereto as **Exhibit "15"**. Tunç sent the notification pursuant to Microsoft's bug bounty program. Tunç holds the following cybersecurity credentials: ISO/IEC 27001 Lead Auditor, GIAC Web Application Penetration Tester (GWAPT), GIAC Certified Enterprise Defender (GCED), and 650-153-Cisco IronPort Security Associate - Email Security (ESFE).

33. Specifically, Tunc informed Microsoft that attackers could bypass Safe Links by using the publicly available IP addresses of Microsoft's EOP servers to know whether to deliver benign or malicious content.

34. On February 24, 2017, Microsoft wrote Tunc: "we have opened a new MSRC case 37595 for this finding and submitted your report for review by our bounty team." *See* **Ex. 15**. Additionally, MSRC sent Tunç the following link that was entitled "Definition of a Security Vulnerability": https://technet.microsoft.com/library/cc751383.aspx. A true and correct copy of Microsoft's "Definition of a Security Vulnerability" is attached hereto as **Exhibit "16."** According to that link, Microsoft represented that it only considered inadvertent weaknesses to be bugs, whereas, "by-design weaknesses" do not meet Microsoft's security bug bar. Specifically, Microsoft stated: "Security vulnerabilities involve inadvertent weaknesses**; by-design weaknesses**

may sometimes occur in a product, but these aren't security vulnerabilities." (emphasis added). *See* **Ex. 16**.

35. On March 15, 2017, Microsoft notified Tunç that "We have completed our investigation and found that this issue doesn't meet security servicing bug bar… We anticipate no further action on this item from MSRC and will be closing out this case. Thanks, Will MSRC." A true and correct copy of the March 15, 2017 email from Microsoft to Tunc is attached hereto as **Exhibit "17."**

36. In doing so, Microsoft conceded that Tunç's observation of Safe Link's susceptibility to dynamic links was a "by-design weakness" and not a fixable bug. Microsoft essentially conceded its knowledge that Safe Links is susceptible to such attacks by its very design.

37. Thus, Microsoft publicly promotes Safe Links as an effective solution to thwarting the malicious use of dynamic links, yet conceded at least to Tunç that Safe Links has a "by-design weakness" that makes it incapable of thwarting the IP Cloaked dynamic links reported by Tunç.

38. In fact, Microsoft continues to promote Safe Links as the answer to malicious dynamic links nearly three years after Tunç notified Microsoft in writing regarding its ineffectiveness against this very attack.

39. Up until now, Microsoft has not modified the design of Safe Links to even attempt to address the all-too-common issue of IP Cloaked links. Rather, Microsoft did exactly as they told Tunç by taking "no further action on this item from MSRC" and "closing out this case," thereby further documenting Microsoft's awareness that Safe Link's lack of protection is inherent in its design and not a fixable bug.

40. It is therefore false for Microsoft to promote Safe Links as a solution to a problem that it was not even designed to address. In the alternative, it is misleading for Microsoft to promote Safe Links as a solution to a problem that it was not even designed to address.

41. Prior to Microsoft offering its Safe Links service, companies generally knew to keep their security on-site to prevent hackers from using IP-cloaked dynamic links to bypass their blacklists, machine learning and artificial intelligence. To convince these companies to purchase Microsoft's ATP service, Microsoft has made false statements to them promising to protect against dynamic links. In fact, Microsoft presents Safe Links' alleged protection against dynamic links as the linchpin of the purchase decision. Microsoft does so by first admitting that attackers can ensure malicious dynamic links bypass the first multi-billion dollar round of detection, and then offers Safe Links as the answer to this problem. Given that no company would willingly make itself defenseless against the most common hacking attack, such marketing, advertising and promotion by Microsoft frames Safe Links as the linchpin and cornerstone of the purchasing decision.

42. In fact, as will be discussed, the industry as a whole presents protection against dynamic links as the linchpin of the purchase decision for email security services. Thus, Microsoft's deceptive advertising is regarding a material quality (if not the most material quality) in terms of the purchase decision.

43. Moreover, Tunç wrote a blog article confirming how "simple" it is for "an attacker" to elude Safe Links with IP-cloaked dynamic links:

> In this article I will go through my findings and analysis on the Safe Links feature of Microsoft's Office 365 Exchange Online Advanced Threat Protection… an attacker could simply block or re-direct requests from the Exchange Online Protection infrastructure – **yup, it's as simple as that** . . . **Helpfully, Microsoft makes the EOP IP ranges available online so all you need to do is block those ranges on your webserver** . . . .

A true and correct copy of the article, found at: https://emtunc.org/blog/03/2017/bypassing-safe-links-exchange-online-advanced-threat-protection/, is attached hereto as **Exhibit "18"** (emphasis added).

44. On August 21, 2018, a free software program for automatically bypassing Microsoft's Safe Links was uploaded to Github (a site with over 32 million monthly visitors). This free program is entitled *mkhtaccess_red*. Microsoft's EOP/ATP IP address ranges come preinstalled in *mkhtaccess_red*'s default configuration file.

45. *Mkhtaccess_red* uses IP cloaking to redirect Microsoft's ATP servers to benign content and to redirect Microsoft's ATP customers to malicious content. Even script kiddies can use *mkhtaccess_red* to evade Microsoft's Safe Links via IP Cloaking.

46. Microsoft has continued to imply that only "sophisticated attackers" use dynamic links to bypass their billion-dollar first round of detection for more than one year after the free availability of *mkhtaccess_red.*

47. Microsoft's implication that only "sophisticated attackers" use dynamic links to bypass their billion-dollar first round of detection is misleading.

48. Apache is one of the most popular webservers. The Apache webserver uses a file called '.htaccess' to redirect listed IP addresses to other sites. *Mkhtaccess_red* inserts Microsoft's IP addresses into the .htaccess file, whereupon the Apache web server redirects Microsoft's scanners to a safe site, making malicious content completely invisible to Microsoft's security service.

49. In December 2018, almost two years after Tunç notified Microsoft regarding Safe Links' lack of defense, Cryptron Security found that hackers can still bypass Microsoft's Safe Links using .htaccess redirects: "…an attacker could simply block or redirect requests from the

Microsoft ATP Safe Links service infrastructure. Microsoft makes the ATP Safe Link IP ranges available online. An attacker needs only to block those IP ranges on the webserver with .htacess rules." A true and correct copy of the article from Cryptron Security is attached hereto as **Exhibit "19."**

50. Approximately two months later, in February 2019, Rhino Security Labs also confirmed that hackers can use dynamic links to bypass Microsoft's Safe Links. (See https://rhinosecuritylabs.com/social-engineering/bypassing-email-security-url-scanning/). Rhino Security Labs is a cybersecurity company that has provided security testing for many large companies. The metadata in the Rhino Security webpage indicates that the content was posted on February 19, 2019. A true and correct copy of the article from Rhino Security Labs is attached hereto as **Exhibit "20."**

51. In August 2019, Tunç performed another test to determine if dynamic links continue to make phishing sites and malware invisible to Microsoft's Safe Links. Tunç's August 2019 report documents that ATP Safe Links continues to be bypassed via IP-Cloaked dynamic links, contrary to Microsoft's public marketing and promotion regarding Safe Links' capabilities - the marketing and promotion that convinced millions to move to the cloud. A true and correct copy of Tunc's August 2019 report is attached hereto as **Exhibit "21."**

52. In Microsoft's current ATP Product Brochure, Microsoft makes the following claim regarding Safe Links: "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." *See* **Ex. 7**.

53. In both its product video and product brochure, Microsoft clearly markets and promotes Safe Links' promised protection against dynamic links as the linchpin of the purchase decision. However, Microsoft's promotion, marketing and advertising of Safe Links, including the referenced statement from its current ATP product brochure regarding Safe Links' protection, is literally false. Alternatively, at a very minimum, Microsoft's promotion, marketing and advertising is misleading, confusing and/or deceiving.

54. After all, Safe Links is bypassed virtually 100% of the time using the simplest, most commonly used form of dynamic links - IP Cloaking.

55. Hackers can even use IP Cloaking to send Microsoft customers to sites that are blacklisted by Microsoft's Safe Links. For illustration, consider a hypothetical site that is actively blacklisted by Safe Links: iamhackingyou.com. IP cloaking can be used to secretly send Safe Links' users to the blacklisted site as follows:

a. The link in the email points to a non-blacklisted domain with a benign name.

b. When Microsoft's security service connects to the link, the link redirects the service to a safe site (such as bankofamerica.com).

c. Microsoft's security service approves the link because it only sees good content from a good site.

d. Microsoft's security service communicates to its customer's device that it is okay to access the now-approved link.

e. When the customer's device accesses the approved link, the link redirects the customer's device to iamhackingyou.com.

f. Microsoft's security service is not even aware that its customer was sent to the blacklisted site.

g. The user does not know that he was sent to a blacklisted site.

h. Nevertheless, the user is now harmed because Safe Links sent the user to a site that was on its blacklist.

56. Thus, as shown above, Microsoft's Safe Links' security is easily defeated by dynamic links, the very attack Microsoft promises that Safe Links protects against.

3. Deceptive Message #2: Attackers Redirect to Unsafe Sites via a Forwarding Service After the Message Has Been Received; But with Safe Links, Malicious Links are Dynamically Blocked while Good Links Remain Accessible.

57. Microsoft markets, promotes and advertises ATP and Safe Links with the following statement:

> …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. (emphasis added)

See 2015 ATP Product Guide (**Ex. 3**), 2016 ATP Product Guide (**Ex. 4**), 2017 Office 365: Everything You Wanted to Know (**Ex. 12**), and 2019 ATP Partner Datasheet (**Ex. 13**) (emphasis added).

58. Microsoft has been delivering this message for four years from the launch of ATP in 2015 (**Ex. 3**), 2016 (**Ex. 4**), 2017 (**Ex. 12**), up to the present (**Ex. 13**). Specifically, for four years, Microsoft has promised Safe Links' protection against dynamic links whose malicious content is cloaked "by a forwarding service."

59. At the time Microsoft launched its ATP offering, IP-Cloaked forwarding services were "widely used by attackers to 'cut the attack chain' in the face of a security scanner." For example, ProofPoint's 2014 Analysis of a Cybercrime Infrastructure provides:

> In order to avoid detection, **it is *common practice* for attackers to add a layer of redirection, known as a Traffic Distribution Service (TDS).** Originally used to route web traffic, TDS's have been *widely used* by attackers as a means to "cut the attack chain" in the face of a security scanner.
>
> **The TDS will only lead visiting browsers into loading exploits if it has verified that the client is neither a crawler nor a security scanner**, and that an exploit is indeed available for the visiting browser. **This technique is sometimes referred to as "cloaking"; since the visiting IP address plays a significant role in this decision process, it can also [be] referred to as "*IP cloaking*."**
>
> **Today, cybercrime groups often offer TDS's as a service. . . . From March 4 to the present, they switched to using Sutra TDS, which is a powerful TDS that has been *popular* among cybercrime groups in order to cloak IP addresses and circumvent detection** (Screenshot 8).

A true and correct copy of Analysis of a Cybercrime Infrastructure by Proofpoint Researchers is attached hereto as **Exhibit "22."** (emphasis added).

60. Currently, hackers continue using IP-Cloaked forwarding services to redirect "to unsafe sites" "after the message has been received." Current examples include justcloakit.com and cloakerly.com.

61. IP Cloaking is the most commonly used tactic of malicious users of forwarding services.

62. To unambiguously promise that Safe Links protects against dynamic links in the context of forwarding services is literally false. Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

63. Microsoft's promotion also contains a categorical promise of protection. Specifically, Microsoft promises protection every time a user clicks a link so that [category 1] malicious links are dynamically blocked while [category 2] good links can be accessed. Microsoft's promotion promises specific outcomes based on two categories: malicious links vs. good links.

64. By presenting the protection categorically, Microsoft is promising that all malicious links are dynamically blocked while all good links can be accessed.

65. Microsoft makes these categorical assertions within the context of an industry in which, as will be explained below, other vendors make absolute guarantees regarding the effectiveness of time-of-click redirection in regards to malicious dynamic links. Therefore, in context, Microsoft is indeed making the literal categorical assertion that all malicious links are dynamically blocked while all good links can be accessed.

66. This categorical assertion of Safe Links' protection is literally false. Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

67. Alternatively, this categorical assertion within the context of forwarding services is literally false. Alternatively, at a very minimum, this categorical assertion within the context of forwarding services is misleading, confusing, and/or deceiving.

4. Deceptive Message #3: You Don't Need Any Other Security Products. With ATP You're Covered.

68. Microsoft's primary promotional webpage for its Advanced Threat Protection service is located at https://products.office.com/en-us/exchange/advance-threat-protection. See excerpt of topmost portion (**Ex. 2**).

69. Microsoft uses the URL in the above paragraph for commercial advertisement of ATP, as evidenced by, among other things:

a. a "Plans & pricing" menu option at the top menu;

b. a "Buy Office 365" button also in the top menu;

c. a "SEE PLANS AND PRICING" button in the topmost content area;

d. On August 13, 2019, an analysis conducted on this URL revealed that 229 different domains contain a total of 1,045 links pointing to this URL. An excerpt of this

backlink analysis is included as **Exhibit "23."** This analysis documents that domains with millions of visitors per month use this specific URL to direct their visitors for the promotion of ATP. For example:

i. BleepingComputer.com says "Millions of visitors come to BleepingComputer.com every month to learn about the latest security threats, technology news, ways to stay protected online, and how to use their computer more efficiently." Bleepingcomputer.com connects prospective customers for "Office 365 ATP" to this specific URL.

ii. TechRepublic.com has 36.7 million unique visitors monthly, and it connects prospective customers for "Office 365 Advanced Threat Protection" to this specific URL. *See* **Ex. 23**; and

iii. On August 9, 2019, a Google search was conducted using the following: purchase Microsoft advanced threat protection. This URL is the first result returned in the search (excluding advertisements). A true and correct copy of the Google search result is attached hereto as **Exhibit "24."**.

70. The webpage located at the subject URL ties together the ATP Product Brochure (**Ex. 7**), and the Office 365 ATP Case Study (**Ex. 9**).

71. Only one case study is referenced by Microsoft on its primary promotional ATP webpage, which is titled "Office 365 ATP case study." A true and correct copy of such case study is attached hereto as **Exhibit "25."** This case study includes the following quote: "We no longer have to worry about what security product we'll use. With Microsoft 365 we're covered."

72. Though the quote was originally supplied by a customer, Microsoft

a. Made the letters of the quote larger than the letters used in the body of the case study;

b. Put a space before and after the quote to isolate it from the body;

c. Used a different color to draw attention to the quote;

d. Used this quote as the first callout in the case study;

e. Chose this to be the sole case study on the ATP promotional page; and

f. Uses this same quote, in isolation, on other promotional webpages including Microsoft's Enterprise-Class Technology webpage (**Ex. 10**) and Microsoft's Optimize Security with Minimal Complexity webpage (**Ex. 11**).

73. Through the above actions, Microsoft promotes the message that no other security products are needed because, with Microsoft's ATP security, companies are covered.

74. Microsoft's promotional message that Microsoft's ATP security is all that is needed is literally false. Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

75. Additional documentation regarding Microsoft's promoting the message that its security is all a company needs is identified below.

5. Deceptive Message #4: Safe Links.

76. The very name "Safe Links" conveys that Microsoft's security service makes links "safe."

77. Microsoft promotes the name "Safe Links" as a service that *guarantees* hyperlinks are harmless: i.e., "ensure hyperlinks in documents are harmless with ATP Safe Links." *See* **Exs. 5, 6 and 14**. In this repeated messaging, Microsoft equates the name "Safe Links" with "ensure hyperlinks in documents are harmless."

78. The word "ensure" means "to make certain; to guarantee."

79. As will be explained below, other popular cybersecurity vendors falsely portray time-of-click redirection as "ensuring" safety so that users "never" visit malicious sites. Thus, within the context of the industry as a whole, Microsoft's prospective customers would understand Microsoft to be guaranteeing safety through its use of the word "ensure."

80. Given Safe Links' by-design inability to thwart the most commonly used cloud attack (IP Cloaked dynamic links), it is literally false to convey the message "Safe Links." Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

81. A product name violates the Lanham Act when the name misrepresents a material quality of the product, most especially when the defendant has been engaged in deceptive advertising regarding that material quality.

82. Here, Microsoft has been engaged in a highly successful deceptive advertising campaign regarding the core quality of 'safety' in its Safe Links service. This false advertising regarding the material quality of safety has produced a false association between the name "Safe Links" and the false claims of safety. In the alternative, this misleading advertising regarding the material quality of safety has produced a misleading, confusing and/or deceiving association between the name "Safe Links" and the false claims of safety.

83. Deceptive advertising regarding the safety of an offering is not a matter of mere puffery. Rather, it is a traditional claim of consumer misrepresentation.

84. In regards to cybersecurity products and services, the quality of safety is not just a material quality. Rather, it is the core quality that consumers consider when making a purchase decision. Therefore, any misrepresentation of the safety of a cybersecurity product or service is a misrepresentation of a material quality of that product or service.

6. False Message #5: Safe Links Ensures Hyperlinks in Documents are Harmless.

85. Microsoft created power point presentations that are to be used for the marketing and promotion of ATP. See reduced images from slides of PowerPoint presentations of Microsoft's Office 365 ProPlus Pitch Deck attached as **Ex. 5** and Microsoft's Office 365 ProPlus Mac Pitch Deck attached as **Ex. 6**. All slides are intended to be shown to customers except for slide 1. Slide 1 indicates that these PowerPoint presentations are to be used when presenting to Business Decision Makers, Technology Decision Makers, and IT Decision Makers ("Audience: BDM, TDM, ITDM"), the "CORE content" is "slides 2-28," the presentations contain "approved messaging," and "Messages and wording have been reviewed by stakeholders."

86. In the "CORE content" of the power point presentations, Microsoft provides approved messaging to promote and market to decision makers that its security "ensure[s] hyperlinks in documents are harmless with ATP Safe Links." *See* **Ex. 5**, p. 22; **Ex. 6**, p. 20. Microsoft also makes nearly the identical representation in its 2019 "Exchange Online Business Class Email System" brochure. *See* **Ex. 14** ("Ensure document hyperlinks are harmless with ATP Safe Links.").

87. However, the statement that Safe Links *ensures* hyperlinks in documents are harmless is literally false. Alternatively, at a very minimum, it is misleading, confusing and/or deceiving. As discussed in detail above, Safe Links can be easily bypassed by IP cloaking and, thus, Safe Links does not *ensure* that hyperlinks are harmless.

88. Both PowerPoint presentations attached as **Exs. 5 and 6** were finalized more than 9 months after Tunç notified Microsoft of Safe Links' susceptibility to IP-Cloaked Dynamic Links.

89. A Google search result demonstrates that both PowerPoint presentations were publicly retrievable from the following site: https://o365pp.blob.core.windows.net. Azure's cloud

storage system uses the following URL convention: https://*mystorageaccount*.blob.core.windows.net. Thus, the Pitch Decks were uploaded by the owner of the Azure cloud storage account entitled 'o365pp.' The owner of 'o365pp' entitled the file name "Office 365 ProPlus Overview for Decision Makers Speaker Notes.docx." A true and correct copy of the Google search result is attached hereto as **Exhibit "26."**

90. Another Google search result demonstrates that the PowerPoint presentations were not accessible to the general public on August 11, 2019. A true and correct copy of the subsequent Google search result is attached hereto as **Exhibit "27."**

7. Consumer Surveys, Market Research and Case Studies.

91. No evidence of deception is necessary to satisfy any of the allegations of literally false representations. Consumer surveys, market research, expert testimony, or other evidence can be used to support allegations of misleading, confusing and deceiving representations.

92. Consumer surveys document that Microsoft's deceptive promotion of its Advanced Threat Protection service (including Safe Links) have misled purchasers regarding its security capabilities.

93. Market Research reports document that Microsoft's deceptive promotion of its Advanced Threat Protection service (including Safe Links) have misled purchasers regarding its security capabilities.

94. Case Studies document that Microsoft's deceptive promotion of its Advanced Threat Protection service (including Safe Links) have misled purchasers regarding its security capabilities.

95. In 2015, IP Cloaking was the most commonly used method for consistently bypassing cloud-based security. In "Next Generation Of Exploit Kit Detection By Building

Simulated Obfuscators," Tongbo Luo and Xing Jin stated: "In this paper, we tracked and collected over 20000 obfuscated JavaScript samples of 5 exploit kit families from 2014 to 2016. . . Nearly every exploit kit leverages various evasion techniques (e.g. IP cloaking, DGA), which makes consistently sample collecting quite challenging." A true and correct copy of Next Generation Of Exploit Kit Detection By Building Simulated Obfuscators" by Tongbo Luo and Xing Jin is attached hereto as **Exhibit "28."**

96. In 2015, Microsoft began promoting Safe Links as an effective solution to the central cloud security issue of IP Cloaked forwarding services.

97. In 2015, security was the number one challenge for convincing consumers to move to the cloud: "Security remains the top adoption challenge . . . ." A summary of 2015 IDG Enterprise Cloud Computing Study posted at https://www.idg.com/tools-for-marketers/2015-cloud-computing-study/ is attached hereto as **Exhibit "29."**

98. Just two years into Microsoft's marketing campaign, by 2017, consumer perception had completely reversed: "Security concerns have traditionally ranked among the top inhibitors of cloud adoption. But in a striking reversal, security has now become a key reason businesses choose cloud solutions, according to a global survey of more than 500 IT decision-makers. . . ." A summary of 2017 MIT SMR Customer Study posted at https://cloud.withgoogle.com/build/infrastructure/whats-behind-growing-confidence-cloud-security/ is attached hereto as **Exhibit "30."**

99. Within four years of Microsoft's marketing campaign, by 2019, over 98% of Microsoft's cloud-based customers at least considered the possibility that Microsoft's security "is sufficient" in and of itself. The survey asked decision makers who use Office 365, "Do you think the current security protection for Office 365 is sufficient?" Only 1.96% answered "definitely not."

A true and correct copy of Organizational Security & Compliance Practices in Office 365 is attached hereto as **Exhibit "31."**

100. The majority of cloud growth from 2015-2019 was driven specifically by the adoption of Microsoft's cloud-based Office 365. A true and correct copy of Cloud Adoption 2018 War by Bitglass is attached hereto as **Exhibit "32."**

101. Prior to Microsoft offering its Safe Links service, consumers were safe from IP Cloak forwarding services when they used on-site security. Microsoft knowingly made companies defenseless to this widely-used, highly-effective, stealthy attack in order to procure billions of dollars in sales.

102. According to Microsoft, it is imperative for Microsoft to be perceived as a leader in security to convince enterprises to purchase its cloud-based apps: "Microsoft is making tremendous investments in data security and compliance… because they understand that to convince enterprise customers… the company needs to be a leader in security and compliance." **Ex. 31.**

103. Microsoft's 2018 Q4 Form 10-K confirms that perception of its security is inextricably tied to purchase decisions:

> "**The security of our products and services is important in our customers' decisions to purchase or use our products or services**. . . . If we fail to do these things well, actual or **perceived security vulnerabilities in our products and services**, data corruption issues, or reduced performance **could harm our reputation and lead customers to reduce or delay future purchases of products or subscriptions to services, or to use competing products or services**."

A true and correct copy of Microsoft's 2018 Q4 Form 10-K is attached hereto as **Exhibit "33."** (emphasis added).

104. Microsoft's own Case Studies regarding its leading partners document that perception of Microsoft's ATP security is an essential element of the purchase decision. For

example, Microsoft's Partner Profile of Olive + Goose demonstrates that Microsoft's deceptive security messaging is central to *every Office 365 engagement*: "'Every Office 365 engagement that we're a part of has a component of security discussion or deployment and implementation with a customer…' Advanced Threat Protection (ATP) in Office 365 Enterprise E5 offers a compelling customer story." A true and correct copy of the Olive + Goose Case Study is attached hereto as **Exhibit "34."**

105. According to that study, "Olive + Goose is a leading IT solutions company, with a wide base of customers in the US and worldwide."

106. Additionally, Microsoft's "Peters & Associates" Partner Profile documents that Microsoft's ATP security is *selling like hot cakes, number one on their list*:

> Ward highlights Microsoft's Advanced Threat protection (ATP) as one of the key launch points for bundling opportunities. '**ATP is selling like hot cakes, it's number one on our list**,' Ward said. . . . Ward explained that security is one of the key components reshaping their practice. Security sells. . . . As evidence, Ward described the sales cycle for a 2500-seat organization that needed a Cloud Application Security Broker (CASB) to support their work with the insurance industry. Because Microsoft Cloud App Security is deeply integrated into Office 365, Peters & Associates could structure a sale around what Ward calls the "5-5-5 program, involving Office 365 E5, EMS E5, and Windows 10 E5.

A true and correct copy of the Peters & Associates Case Study is attached hereto as **Exhibit "35."**

107. According to that study, "Chicago-based Peters & Associates provides full-service IT consulting, managed IT services, and integrated IT solutions… They have a long record of success as a Microsoft Partner."

108. As both Olive+Goose and Peters & Associates document, Microsoft profits not only from the sale of ATP security itself, but Microsoft's promotion of ATP security is also essential to procuring the majority of sales of Office 365, which is Microsoft's most successful product offering in history.

109. These studies document that consumers are moving to Microsoft's cloud directly due to trusting Microsoft's deceptive promotions regarding the security of Microsoft's ATP security service.

110. In fact, Microsoft's deceptive advertising is causing companies to abandon third party solutions in order to consolidate their security with Microsoft's ATP service - ATP Safe Links specifically:

> While most federal agencies have relied upon dedicated security solutions that require expensive subscriptions and costly hardware, they're finding that agencies are receptive to **Microsoft security solutions as a *fully capable***, less costly ***alternative***. 'These agencies realize they're spending tens of thousands of dollars a year on security subscriptions, not to mention the hardware costs,' explained Jeff Fowler, Federal Senior Cloud Strategist for Planet Technologies. "If they can get **Advanced Treat Protection (ATP)** and other Office 365 security tools that provide the same functionally **at a lower price point than what they are *paying for their current solutions, they're going to jump* at the opportunity." . . .**
>
> As Fowler relates, 'IT management at the federal customer wondered, 'Why are we paying for our current bolt-on security product when ***we can get similar functionality from Microsoft built-in*** for just a couple more bucks per user?' **That made the decision to deploy ATP a nobrainer.' Advanced Threat Protection (ATP) is one of the specific reasons the agency decided to *switch*. 'Using ATP, we've enabled Safe Links** across the entire tenant with about 1,000 users now, and Safe Attachments is currently being trialed,' Fowler said.

A true and correct copy of the Planet Technologies Case Study is attached hereto as **Exhibit "36."**

111. According to that study, "Planet Technologies is a successful Microsoft partner with significant experience in cloud and datacenter services, cyber security, and mobile application development…. Planet Technologies is a 6-time Federal Partner of the Year, 6-time State & Local Government Partner of the Year, and 5-time Windows Partner of the Year."

112. The case study above is representative of a current trend of companies getting rid of third-party security in order to *consolidate* by using Microsoft's security alone.

113. Additionally, Microsoft commissioned a study by Forrester Consulting titled "Total Economic Impact™ Of Microsoft Office 365 Threat Intelligence." This study documents that Microsoft is successfully deceiving companies *en masse* into believing they can swap their third-party security for Microsoft's "end-to-end cyber protection": "*Prior to deploying Office 365 E5* with Threat Intelligence, *the interviewed and surveyed customers typically used many disparate third-party solutions to handle email and data file protection*, resulting in complex security environments that were both expensive and difficult to manage… This integrated suite of security products provides a holistic approach to security, *providing end-to-end cyber protection*." A true and correct copy of "The Total Economic Impact™ Of Microsoft Office 365 Threat Intelligence" is attached hereto as **Exhibit "37."**

114. Microsoft's deceptive message of the full sufficiency of its security offering is deceiving a large number of organizations: "*With the deployment of Office 365 E5, organizations can consolidate their security solutions onto a single platform*, reducing licensing costs expended on a myriad of third-party security solutions." See **Ex. 37.**

115. The study has the following disclaimer: "This study is commissioned by Microsoft and delivered by Forrester Consulting… Microsoft reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study… Microsoft provided the customer names for the interviews but did not participate in the interviews." See **Ex. 37.**

116. As is customary with commissioned consulting reports, the report is only issued upon the approval of the purchaser, Microsoft in this case, making the commissioned report a promotional marketing piece approved by and distributed by Microsoft.

117. Microsoft's case studies, partner profiles, and commissioned consultancy reports collectively promote the message of abandoning third-party security in order to consolidate into Microsoft's offering alone.

118. Microsoft's case studies, partner profiles, and commissioned consultancy reports also document Microsoft's success in deceiving consumers *en masse* to consolidate their security with Microsoft's platform – all while Microsoft knows its platform has a "by-design weakness" that allows its security to be bypassed, in its entirety, via IP Cloaking.

119. Security is a higher priority than compliance: "…security is more prioritized because the effects of security failings are costlier than the effects of compliance failings." (See **Ex. 31**).

D. TocMail as Sole Provider.

120. By 2011, IP Cloaking had already become the most effective form of evasion, as it thwarts any sort of detection. See **Ex. 1**. As reported by Rhino Security Labs, IP Cloaking continues to this very day "to bypass known sandbox and threat protection providers" – not just Microsoft's cloud-based security services. *See* **Ex. 20**.

121. TocMail's CEO invented a solution and obtained a patent on the first technology that enables a cloud-based redirection service to consistently thwart malicious use of dynamic links (United States Patent No. 10,574,628 ("'628 Patent")). TocMail's CEO assigned all patent rights to Plaintiff.

122. Prior to Plaintiff's patented technology, no company provided a URL redirect security service capable of thwarting IP-Cloaked dynamic links.

123. Prior to Plaintiff's patent, every cloud-based URL redirect security service operated as follows:

a. The security service follows the path of the original URL.

b. The security service assesses the security of all URLs in the path (often including assessing the content delivered by the final URL).

c. If no security threats are seen, the security service exits by sending the user's device to the original URL – which can now take them anywhere it wants.

124. The "by-design weakness" in Microsoft's Safe Links and all other competitors was the last step where the security service exits by sending the user's device to the original URL, which can now take them anywhere it wants.

125. A service cannot claim to protect consumers from malicious use of dynamic links when that service's final act is to hand control over to the dynamic link itself. However, this is precisely the situation at hand with Microsoft's Safe Links and all competitors, with the sole exception of Plaintiff.

126. Plaintiff finally solved the central issue of cloud security (IP Cloaked redirects) by doing the following:

a. The security service follows the path of the original URL.

b. The security service assesses the security of the final domain and final URL in the path.

c. If no security threats are seen, the security service exits by sending the user's device **straight to the final site - bypassing the original URL altogether.**

127. Only in Plaintiff's technology are users consistently sent to the same site that the security service assesses. With Safe Links and others, the security service might assess a site that is safe, but the user is then sent to a malicious site that the security service never even assessed.

128. Plaintiff's technology does not have the 'by-design weakness' of handing control back to the original URL, when dynamic redirects are used.

129. Moreover, Plaintiff's '628 Patent now legally bars its competitors from sending users anywhere other than the original URL. For any company that assesses the final site in a redirect path, Plaintiff's patent requires them to go to the original URL. Since other companies are restricted to going to the original URL, they remain defenseless against the most common cloud hacking attack (until Plaintiff's patent expires).

130. Thus, Plaintiff is the sole provider of a cloud-based URL redirect security service that thwarts malicious use of dynamic redirects.

131. There is no need to speculate regarding the number of professionals willing to subscribe to a cloud-based redirect service that offers protection against malicious use of dynamic links, as approximately 100 million have already demonstrated their willingness by purchasing Microsoft's cloud-based service, which was promoted expressly as providing protection against malicious dynamic links.

132. There is no need to speculate on how many of these professionals would have chosen Microsoft in the absence of false advertising given that no professional would willingly make themselves defenseless against the very attack that they are purchasing protection from.

133. There is no need to speculate how many professionals would have chosen Plaintiff given that Plaintiff is the sole provider of that which they have demonstrated their willingness to buy.

134. There is no need to speculate on the amount of money that would be spent by purchasers of Plaintiff's service given that companies already spend billions per year intending to purchase this very service from Microsoft.

135. IP Cloaking had been the most effective method for bypassing cloud-based security for a decade.

136. Despite offering the only cloud redirect service that solves this all-important issue, Plaintiff cannot sell its service to those that already expressed billions of dollars of intent on purchasing this service because they wrongly believe they are already getting this service from Microsoft.

137. Upon information and belief, Microsoft currently has approximately 93,744,000 consumers relying on Safe Links, which was calculated by Microsoft's overall Office 365 user base times the percentage of those users that use Safe Links as documented in the consumer survey co-sponsored by Microsoft. *See* **Ex. 31**.

138. Based on Microsoft's growth since the above-referenced report, more than 100 million professionals withhold trade from Plaintiff due to Microsoft's deceptive practices. This represents an annual lost revenue of over $3 billion to Plaintiff ($43 billion over the lifetime of the patent).

139. The mere cessation of false advertising will not come close to preventing future injury to Plaintiff caused by Microsoft because Microsoft has already convinced these purchasers to trust its security and does not need to continue the false advertising campaign to retain them.

140. Given that no other company developed a cloud-based redirect service capable of protecting against this common attack *for more than a decade*, and given that Plaintiff's patent restricts all competitors that assess final destinations to sending their users to the original URL, Plaintiff is destined to remain the only provider of a cloud-based redirect service immune to this attack until Plaintiff's patent expires on May 7, 2035. Plaintiff will have suffered damages from Microsoft's false advertising during this entire period, and is therefore seeking just relief.

141. The sole provider of a product or service is inherently damaged when a competitor capitalizes on consumers' desire to purchase that offering by falsely claiming to provide the same. Likewise, proximate causation of harm inherently exists when a competitor uses false or misleading advertising to influence purchase decisions regarding an offering that a plaintiff alone provides.

E. Contributory False Advertising.

142. Microsoft not only harms Plaintiff through its own false advertising but also harms Plaintiff through contributory false advertising as well.

143. Multiple third parties offer alternatives to Safe Links to protect Microsoft Office 365 users. Microsoft benefits significantly when consumers choose to subscribe to Microsoft's cloud services out of trust in a third-party's security offering.

144. Microsoft provides many of these third parties access to its customers' accounts via a proprietary protocol. Such third parties cannot offer their services without Microsoft providing access.

145. Microsoft also has other technology partnerships and relationships designed to foster adoption of Microsoft cloud apps even when such apps are secured by a third-party. Microsoft benefits greatly from its contributory role in the false advertising of third party security vendors that make Microsoft's cloud apps appear to be safe.

146. Almost all email cybersecurity vendors participate in a coordinated, industry-wide deception that promotes 'time-of-click' redirection as the solution to links that appear benign to cloud scanners yet send users to somewhere dangerous. The industry further promises that time-of-click security makes cloud computing just as safe (if not safer) than on-premise computing.

This coordinated deceit is the very basis for the rise in cloud adoption, resulting in the vast majority of companies now being effortlessly (and secretly) hacked at will.

147. The following deceptive advertising from Sophos is emblematic of the industry-wide campaign to convince companies to move to the cloud under the false promise of security: "Simply secure Microsoft Exchange, Office 365, and Google Apps[:] **Shifting your email to the cloud doesn't mean you have to reduce your security.**" See "Sophos Email," which is attached hereto as **Exhibit "38."** (emphasis and punctuation added).

148. Sophos is advertising its cloud-based email security service. It deceptively claims its time-of-click service protects against email links that attempt to deliver malware only after the email has reached the inbox: "Block Stealth Attacks[:] Protecting employees from malicious website links, our advanced URL protection is out-smarting attackers who slip phishing URLs past traditional gateways - delaying the upload of malware to websites until after the email is delivered. Sophos Time-of-Click checks website reputation before delivery and at the time you click – blocking stealthy, delayed attacks." See a second "Sophos Email," which is attached hereto as **Exhibit "39."** (punctuation added).

149. Sophos portrays its time-of-click service as "advanced" protection that's "out-smarting attackers" by blocking "stealthy" attacks. However, like all traditional time-of-click redirect services, it is utterly defenseless against the most common method hackers use to delay their exploits: IP Cloaking. Sophos' promotion of its time-of-click protection is false. Alternatively, Sophos' promotion of its time-of-click protection is misleading, confusing and/or deceiving.

150. Sophos offers its time-of-click protection to Microsoft Office 365 users. Microsoft benefits when Sophos' deceptive advertising convinces companies to subscribe to Microsoft's cloud apps.

151. Contributory false advertising was the basis of Microsoft's Office 365 initial foothold in cloud computing. In October 2010, Microsoft announced that it was going to launch its cloud-based Office 365. In December 2010, Mimecast proudly announced its accelerated accreditation of becoming a Microsoft Gold Partner in only six weeks, allowing it to integrate tightly with Microsoft's email. General availability of Microsoft Office 365 came in 2011, the same year in which Microsoft's Gold Partner Mimecast promoted cloud security as being *superior* to on-premise: "The cloud isn't just *the most effective place to secure email*, before any threats or intruders ever reach your network; it's also the most efficient. Cloud-based email services can offer *full protection* with the promise of availability and reliability too." A true and correct copy of "Security-as-a-Service: Threat mitigation from the cloud" by Mimecast is attached hereto as **Exhibit "40."** (emphasis added).

152. Mimecast offers security protection for Microsoft's Office 365 customers: "Mimecast Broad Spectrum Email Security for Office 365: A cloud-based email security layer for Office 365 that reduces risk and combats targeted threats in email." A true and correct copy of "Mimecast Broad Spectrum Email Security for Office 365" is attached hereto as **Exhibit "41."**

153. Mimecast's protection for Office 365 uses "URL Protect" to address malicious use of dynamic links. Just like Microsoft does for Safe Links, Mimecast also claims that its time-of-click security "ensures" the safety of email links. Mimecast's primary promotional video for its time-of-click service begins as follows: "Mimecast Targeted Threat Protection. URL Protect rewrites all links in inbound emails and **scans destination websites in real time *ensuring***

malicious websites are blocked whatever the device or network used." (emphasis added). Mimecast currently displays this video on its primary Targeted Threat Protection promotional webpage: https://www.mimecast.com/products/email-security-with-targeted-threat-protection/.

154. The video continues on to state that, if the link is deemed to be safe, the user is given access to the original URL. By sending the user to the original URL, Mimecast's URL Protect is utterly defenseless against IP Cloaking - the most common method hackers use to bypass cloud-based security. Thus, it is literally false for Mimecast to claim to *ensure* malicious websites are blocked. In the alternative, it is misleading, confusing and/or deceiving for Mimecast to claim to *ensure* malicious websites are blocked.

155. Given Mimecast's vulnerability to IP Cloaking, it is also literally false to promise that users' destination websites are scanned in real time. For example, a malicious link that sends Mimecast's scanner to bankofamerica.com (safe site) could then send Mimecast's users to iamhackingyou.com (malicious site). In this all-too-common scenario, the user's destination website (iamhackingyou.com) is not scanned in real time. In fact, it is not scanned at all. Even worse still, Mimecast would not even know that the user went to iamhackingyou.com (malicious site).

156. It is literally false for Mimecast to promise it "scans destination websites in real time." In the alternative, it is misleading, confusing and/or deceitful for Mimecast to promise it "scans destination websites in real time."

157. The industry as a whole falsely promotes the following cause/effect relationship: time-of-click redirection makes dynamic links harmless. Cybersecurity vendors make billions of dollars annually by promoting this patently false cause/effect relationship.

158. For example, it is literally false for Mimecast to promote this cause/effect relationship: scanning of destination websites in real time (the cause) ensures malicious websites are blocked (the effect). The conveyance of this cause/effect is literally false. In the alternative, the conveyance of this cause/effect is misleading, confusing and/or deceptive.

159. The industry as a whole also promotes the false promise that time-of-click services assess the same destination that the user will visit. As explained above, this is patently untrue. Microsoft not only plays a contributory role in others that promote this message, Microsoft itself also promotes this deceptive (and dangerous) message.

160. For at least the last year, whenever a person conducted a Google search on 'how Safe Links Works,' the first result from the search was the following Microsoft link: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-atp-safe-links-works. In fact, this page is titled "How Office 365 ATP Safe Links works." A true and correct copy of a printout from the link is attached hereto as **Exhibit "42**." The page states: "ATP Safe Links feature immediately checks the URL before opening *the* website. . . . If the URL is determined to be safe, *the* website opens." (emphasis added) Thus, Microsoft unambiguously states that there is one website (*the* website). However, when it comes to the most-commonly used cloud hacking attack, this is not true. The scanner goes to one website while the user goes to a very different website. Microsoft's language falsely conveys that the scanner will assess the same website that the user will visit - *the* website.

161. One of the most popular cybersecurity vendors is Symantec. Symantec also sells a time-of-click security service for Microsoft Office 365 users. Symantec promotes its service as follows: "*Click-Time URL Protection* blocks malicious links by analyzing them when they are clicked by end-users to *protect against spear phishing attacks that weaponize a link after an email*

is delivered… Unlike other solutions that rely on reactive blacklists or signatures to stop spear phishing attacks, Symantec proactively stops both new and known spear phishing attacks that employ malicious links by performing deep evaluation of links in real-time. *This deep evaluation follows links to their final destination*…" See "Symantec Email Threat Detection and Response" Data Sheet, attached hereto as **Exhibit "43."**

162. As with the other vendors offering protection for Microsoft cloud users, Symantec promotes the same false cause/effect relationship: time-of-click security (the cause) stops links that only lead to malicious content after delivery (the effect). However, any time-of-click service that hands control over to the original URL remains defenseless against IP cloaking; not one bit better than having no time-of-click security at all. There simply is not any cause/effect relationship. Symantec's promotion of this cause/effect is literally false. In the alternative, Symantec's promotion of this cause/effect is misleading, confusing and/or deceitful.

163. Symantec also promises that "deep evaluation follows links to their destination" - conveying that the deeply evaluated destination is the same destination that the user will visit. But when it comes to the most commonly used cloud-based hacking attack, this simply is not true. To promote the idea that Symantec will deeply evaluate the same destination that the user will visit is false. In the alternative, to further promote the idea that Symantec will deeply evaluate the same destination that the user will visit is misleading, confusing and/or deceptive.

164. Just like Microsoft and Mimecast, Symantec claims that time-of-click security *guarantees* (ensures) that users only go to safe sites: "The Click-time URL Protection service 'rewrites' and performs checks on URLs in emails that are delivered to your organization's end users. The process of rewriting allows the service to manage access to the URL to ***ensure*** **the destination is innocuous**. Any URL that is rewritten by Click-time URL Protection is checked

every time an end-user clicks on it, to ***ensure*** **the URL destination is not hosting malware, phishing, or spam threats**." See Symantec's "Product Updates Symantec Email Security.cloud," attached hereto as **Exhibit "44."** (emphasis added).

165. All three vendors promote a service that is utterly defenseless against the most-commonly used cloud hacking attack while *guaranteeing* safety against this very attack. When Microsoft users hear Microsoft promoting the same false message as other leading cybersecurity vendors, they naturally conclude that the popular security vendors are telling them the truth (and that Plaintiff's startup company must be in error). The damage being done to Plaintiff's reputation is incalculable.

166. Proofpoint is a cybersecurity vendor that once strongly warned companies about the danger of IP Cloaked forwarding services in 2014. (See **Ex. 22**.) ProofPoint's warning was quite extensive, including a thorough analysis into how the services work, why they are so dangerous, and the identity of the major players. Today, Proofpoint offers its "URL Defense" service to address the issue of malicious dynamic links.

167. Proofpoint states that its URL Defense service operates as follows: "URL Defense protects organizations from accessing known malicious sites by locating and replacing URLs found within the message body with a separate URL. If users click on a known malicious URL instead of being directed to *the original URL* they are instead directed to a page informing that the site is not safe and been blocked." A true and correct copy of the Proofpoint Essentials Administrator Guide is attached hereto as **Exhibit "45."** (emphasis added).

168. Because Proofpoint hands control over to "the original URL," it has the same by-design weakness as Microsoft's Safe Links, making it equally defenseless against IP Cloaking.

169. Even though Proofpoint's URL Defense is bypassed by the most-commonly-used evasion technique and even though Proofpoint demonstrated its expertise regarding IP Cloaking (in its 2014 report), Proofpoint nevertheless promotes its URL Defense as "the only service that effectively detects, catches and analyzes malicious URLs targeting this market." A true and correct copy of the "Proofpoint Essentials URL Defense" is attached hereto as **Exhibit "46."**

170. Proofpoint's promotional message above is false. Alternatively, at a very minimum, it is misleading, confusing and/or deceiving.

171. Proofpoint offers its URL Defense as an alternative to Safe Links for Microsoft's Office 365 users: "Proofpoint Provides Complete Protection for your Office 365 Deployment: Provides complete protection against advanced threats with URL Defense Service and Attachment Defense Service." A true and correct copy of the Proofpoint's "Microsoft Office 365 and Proofpoint" Essentials Administrator Guide is attached hereto as **Exhibit "47."**

172. Proofpoint has ceased warning customers about IP Cloaked forwarding services, and instead promotes an offering that is literally defenseless against these services, all while promising effective protection nonetheless. This is all to the benefit of Microsoft, the largest cloud-based Software as a Service (SaaS) provider.

173. As shown above: Microsoft, Mimecast, and Symantec promote time-of-click redirection as "ensuring" (guaranteeing) safety for Office 365 users. Barracuda is another popular cybersecurity vendor that promotes time-of-click redirection as an absolute panacea for Microsoft Office 365 users: "Link protection redirects suspicious and typosquatted URLs so malware is *never* inadvertently downloaded by recipients." See "Barracuda Essentials for Email Security," which is attached hereto as **Exhibit "48."** (emphasis added). This specific and exact statement of absolute protection is repeated verbatim by multiple Barracuda resellers - specifically when promoting

Barracuda Essentials specifically for Microsoft's Office 365. Such resellers include: Alliance Business Technologies (https://www.abtechnologies.com.au/barracuda-essentials/), Acordis Technology and Solutions (http://www.acordiscorp.com/barracuda-essentials.html), BarraGuard (https://www.barraguard.com.au/Essentials-Office-365.asp), IT Bus Limited (https://it-b.co.uk/products/essentials-for-office-365/), and OneHQ IT (https://www.fission.co.nz/barracuda-essentials/), and more.

174. Once again, Microsoft benefits from its cloud users being assured that time-of-click redirection guarantees that they will never download malware from a protected link. Such guarantee is false. In the alternative, such a guarantee is misleading, confusing and/or deceptive. Yet such absolute guarantees are highly effective in lulling hundreds of millions of consumers into a false sense of safety, to the degree that they confidently purchase Microsoft's cloud-based apps and services.

175. There are hundreds of millions of hacking attacks, and email security promotional materials are typically short. Thus, it is very telling that Microsoft, Mimecast, Sophos, Barracuda, Symantec and ProofPoint all discuss email links that initially appear to be benign only to lead somewhere malicious after delivery. In fact, Microsoft even openly acknowledges that such emails evade the entirety of its $1 billion per year detection infrastructure. Out of the hundreds of millions of attacks, they all discuss this specific one because promising a solution to this problem is *essential* for convincing companies to purchase cloud-based apps and services. It is material to the purchase decision.

176. As an example, Vade Secure correctly points out security at the time of click is "the most critical step": "With Vade Secure's Anti-Phishing solution, **your users are protected at the**

most critical step: at the time-of-click." See "Anti-Phishing Solution: The Real Time Protection," which is attached hereto as **Exhibit "49."** (emphasis in original).

177. Vade Secure is a cybersecurity vendor that currently protects over 600 million email accounts. It also uses Microsoft's proprietary protocol to integrate with Office 365 user accounts. Hence, Microsoft directly enables Vade's offering.

178. On June 14, 2019, Plaintiff's current CEO sent an email to Vade Secure to see if it too sends users to the original URL just like Microsoft Safe Links does and asked specifically: "What is the advantage of your 'time of click' phishing security vs Microsoft's 'time of click' safe links?"

179. On June 14, 2019, Olivier Saoletti of Vade Secure's Support team responded: "The main difference about "Time Of Click" for Vade Secure and Safe link is that we are using our own databases of malicious URLs. These databases are updated every minute. So you you don't have to create some rules and enter manually some urls to be protected. You can have a look at our website : https://www.vadesecure.com/en/solutions/anti-phishing-2/ And also you can check our antiphishing dedicated website : http://www.isitphishing.org." A true and correct copy of the email chain with Vade Secure is attached hereto as **Exhibit "50."**

180. Given that Microsoft and the rest of the industry passes control to the original URL, if Vade Secure were sending users to a different URL they would have gladly volunteered this revolutionary difference (just as Plaintiff's patented method is a revolutionary difference). However, Olivier Saoletti's response strongly conveys that Vade Secure also sends users to the original URL; thereby being defenseless against IP Cloaking like the rest of the time-of-click industry.

181. Although going to the original URL renders Vade Secure defenseless against IP Cloaking, Vade Secure, who services over 600 email addresses, nevertheless promises that time of click "ensures" safety: "All URLs must be reexamined in real time **to *ensure* that the sites continue to be legitimate, and that they don't redirect to phishing or other types of malevolent sites**." (https://www.vadesecure.com/en/how-can-machine-learning-block-multi-form-attacks/). (emphasis added).

182. The combined impact of all the companies listed in this section affects the perception of approximately 1 billion consumers: Vade Secure protects over 600 million email addresses; Symantec is one of the most popular cybersecurity vendors; Microsoft Safe Links protects approximately 100 million users; and all the other vendors also service numerous mid to large size users.

183. The third parties' false and misleading advertising identified in detail herein is significant for several reasons. First, it elucidates Microsoft's role in contributory false advertising. Second, it provides the essential context in which Microsoft's own advertising is being received and interpreted. Third, it documents the extreme importance of the issue of malicious dynamic links in regards to purchase decisions - so much so that every email security vendor chooses to discuss it (out of the hundreds of millions of other attacks). Fourth, it documents that all of the leading time-of-click redirection providers share the same design flaw (of going to the original URL), making Plaintiff the sole provider of a time-of-click redirection service that actually solves the extremely important issue of malicious dynamic links. Finally, it documents that the approximately 1 billion consumers who have already expressed their desire to purchase that which Plaintiff alone offers are diverted elsewhere through a coordinated false advertising campaign, resulting in extreme damage to Plaintiff's business and reputation.

184. Microsoft continues to supply its service to those it knows or has reason to know are engaged in false advertising directly in regards to the service being supplied. As a result, Plaintiff has been damaged by Microsoft's contributory false advertising.

185. Through its own false advertising combined with contributory false advertising, Microsoft causes approximately 1 billion professionals to withhold their trade from Plaintiff.

186. All conditions precedent to the filing of this action have been fulfilled or waived.

187. Plaintiff has retained the undersigned counsel to represent it in this action and is obligated to pay undersigned counsel's reasonable attorneys' fees, which fees, together with costs, Plaintiff is entitled to recover from the Microsoft pursuant to at least 15 U.S.C. § 1117.

COUNT I
False and Misleading Advertising under 15 U.S.C. § 1125(a)(1)(B)

188. Plaintiff re-alleges and re-avers paragraphs 1-187 as though fully set forth herein.

189. This is an action for false and misleading advertising under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

190. Microsoft has misrepresented the nature, characteristics and/or qualities of its ATP Safe Links service in commercial advertising and/or promotion resulting in Plaintiff being damaged and/or likely to be damaged by such acts. Microsoft continues to misrepresent the nature, characteristics and/or qualities of its ATP Safe Links service in commercial advertising and/or promotion resulting in Plaintiff being damaged and/or likely to be damaged by such act.

191. More specifically, Microsoft's misrepresentations are in regards to the safety of its ATP Safe Links service as described in significant detail above. A claim that a seller falsely represents the safety of its product or service is a traditional claim of consumer misrepresentation.

192. As discussed at length above, Microsoft has made statements of fact in commercial promotion, advertising and marketing that are literally false. Alternatively, at a very minimum,

Microsoft has made statements of fact in commercial promotion, advertising and marketing that are misleading, confusing and/or deceiving. All such statements of fact are found in, among other things, Microsoft's *primary* promotional materials, including but not limited to:

i. the official 2015 EOP ATP Product Guide

ii. the official 2019 ATP Product Guide

iii. the primary promotional webpage for ATP

iv. the PowerPoint presentations designed to be given to key decision makers

v. approved promotional materials to be used by Microsoft Partners

193. Microsoft's actions deceive or have a tendency to deceive the target audience, including consumers and purchasers of its cloud services, and may influence and/or have influenced consumers to refrain from purchasing Plaintiff's service. Additionally, such actions may influence and/or have influenced consumers to purchase Microsoft's service rather than Plaintiff's service. No evidence of deception is required for literally false statements. For misleading, confusing and/or deceiving statements, consumer surveys, market research and other evidence demonstrate that Microsoft's statements are misleading, confusing and/or deceiving.

194. As a result, Microsoft's actions have had and continue to have a material effect on purchase decisions. Among other things, consumer surveys, market research, and case studies discussed above document that Microsoft's deceptive misrepresentations regarding its ATP security had a material effect on purchase decisions not only for the ATP security service itself, but also for Defendant's Office 365. Additionally, Microsoft's 2018 4Q 10K Report also documents that perceptions regarding security have a material effect on purchase decisions. *See* **Ex. 33**.

195. Microsoft has used the subject promotional and advertising materials presented herein to deceptively market its ATP service to millions of consumers in all fifty states, across state lines. Thus, Microsoft's deceptive advertising and promotion affects interstate commerce.

196. Plaintiff is a competitor of Microsoft and has suffered injury to a commercial interest in sales or business reputation proximately caused by Microsoft's misrepresentations. Among other things, Plaintiff has been injured by Microsoft's false and misleading advertising by consumers withholding trade from Plaintiff, presently and in the future due to trusting Microsoft's false advertising. In the alternative, Plaintiff is likely to be injured by Microsoft's false advertising by consumers withholding trade from Plaintiff due to trusting Microsoft's false advertising.

197. Additionally, Plaintiff's business reputation has been injured by Microsoft's false and misleading advertising due to consumers believing that Plaintiff offers nothing of value to them due to their trusting Microsoft's false claims to already be providing the service that Plaintiff provides. Specifically, Plaintiff is the sole provider of that which Microsoft falsely claims to offer, making every dollar gained by Microsoft trade that is being withheld from Plaintiff.

198. Microsoft has deceptively convinced roughly 100 million users to purchase protection from links that appear to be benign, only to change destination when clicked. This deception causes these 100 million professionals to withhold trade from Plaintiff. These professionals also wrongly perceive Plaintiff's security offering as holding no value to them, which irreparably harms Plaintiff's commercial interest and business reputation. Although Plaintiff has solved the single biggest issue in cloud security, Microsoft's misrepresentations have caused it to appear as if Plaintiff claims only to have solved a non-existent problem.

199. The withholding of trade of 100 million professionals results in more than $43 billion in lost profits over the lifetime of Plaintiff's '628 Patent. The mere cessation of false

advertising by Microsoft will not prevent future injury to Plaintiff because Microsoft has already convinced purchasers to trust its security and does not need to continue the false advertising campaign to retain them. Thus, Plaintiff is seeking in excess of $43 billion in damages. Such damages are in addition to the injury to Plaintiff's business reputation.

200. Plaintiff is also seeking an award of Microsoft's profits from both the direct sale of Microsoft's ATP security service and from the sale of Office 365 derived from purchasers trusting Microsoft's deceptive ATP security claims. Disgorgement of ill-gotten profits is separate from and independent of actual damages and is necessary here to deter future conduct and to prevent Microsoft from being unjustly enriched. Among other things, companies were safe from IP Cloaking with their on-premise security, but Microsoft knowingly made companies defenseless against the most commonly used attack in order to procure billions in profit. The worldwide harm inflicted on companies, governmental institutions, and more necessitates future deterrence. There is great public interest in making the misconduct unprofitable.

201. Microsoft's actions described herein have been and continue to be willful, deliberate and intentional. Among other things, as discussed above, in 2017, Microsoft was officially notified that its ATP security can be bypassed in its entirety via IP cloaking, which is the most commonly used evasion technique. Nevertheless, Microsoft continued and still continues to promote ATP Safe Links as effective protection against the very attack that Microsoft knows ATP Safe Links is inherently incapable of thwarting.

202. Microsoft's misrepresentations are causing and will continue to cause damage to Plaintiff including, but not limited to, irreparable harm. Irreparable harm includes the loss of customers and goodwill.

203. Plaintiff is entitled to a temporary and permanent injunction against Microsoft, as well as all other remedies available including, but not limited to, compensatory damages, treble damages, disgorgement of profits, and costs and attorneys' fees. Plaintiff seeks all available remedies.

COUNT II:
Contributory False and Misleading Advertising

204. Plaintiff re-alleges and re-avers paragraphs 1-187 as though fully set forth herein.

205. This is an action for contributory false and misleading advertising under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

206. As discussed above, Microsoft not only harms Plaintiff through its own false advertising but also harms Plaintiff through contributory false advertising as well.

207. Multiple third parties offer alternatives to Safe Links to protect Microsoft's Office 365 users. Microsoft provides these third parties access to its customers' accounts via a proprietary protocol. These third parties cannot provide their services without Microsoft's providing of access, providing technology, and/or providing other forms of assistance. Microsoft provides other cybersecurity companies technology and/or other assistance.

208. As a result of Microsoft's actions, the third parties use promotional and advertising messages that are false. Alternatively, at a very minimum, they are misleading, confusing and/or deceiving. Thus, the third parties are directly engaging in false advertising. Such false advertising injures Plaintiff.

209. Microsoft contributed to the third parties' false advertising by knowingly inducing or causing the third parties' conduct and/or by materially participating in it. Among other things, Microsoft supplies and continues to supply its service to those third parties it knows or has reason

to know are engaged in false advertising directly in regards to the service being supplied. Microsoft is aware that its ATP Safe Links does not protect against the most simple form of attack.

210. By providing access to these third parties in the presence of the false advertising, Microsoft materially benefits and contributes to it.

211. As a result, Plaintiff has been damaged by Microsoft's contributory false advertising.

212. Microsoft's actions described herein have been and continue to be willful, deliberate and intentional.

213. Microsoft's misrepresentations are causing and will continue to cause damage to Plaintiff including, but not limited to, irreparable harm.

214. Plaintiff is entitled to and seeks a temporary and permanent injunction against Microsoft, as well as all other remedies available including, but not limited to, compensatory damages, treble damages, disgorgement of profits, and costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, TOCMAIL INC, prays for judgment against Defendant, MICROSOFT CORPORATION, as follows:

A. Finding Defendant liable for the actions described herein;

B. For temporary and permanent injunctive relief enjoining Defendant and its respective officers, employees, and agents, and all persons or entities in active concert or participation with Defendant, from misrepresenting the safety, nature, characteristics and qualities of its Advanced Threat Protection service and requiring Defendant to take corrective action regarding Defendant's past actions, including Ordering that:

(i) Defendant immediately cease promoting Advanced Threat Protection and/or Safe Links or any of its security services as offering effective protection against the malicious use of dynamic links;

(ii) Defendant immediately cease claiming that its Advanced Threat Protection and/or Safe Links or any of its security services ensure that hyperlinks are harmless;

(iii) Defendant immediately cease promoting Advanced Threat Protection and/or Safe Links or any of its security services as offering effective protection against forwarding services that route to unsafe sites after email messages have been delivered;

(iv) Defendant immediately cease using categorical language to promote the idea that all malicious sites are dynamically blocked;

(v) Defendant immediately cease promoting its security service as fully sufficient and/or the only cybersecurity that a company needs;

(vi) Defendant immediately cease using the deceptive name "Safe Links" for its redirect service;

(vii) Defendant immediately cease its contributory false advertising and requiring all third parties to accurately represent the security they provide to Defendant's customers;

C. For damages, including ordering Defendant to pay Plaintiff monetary relief under 15 U.S.C. § 1117(a) in an amount equal to Defendant's profits, plus damages sustained by Plaintiff in excess of $43 billion, as a result of Defendant's wrongful actions;

D. Ordering Defendant to pay Plaintiff three times Defendant's profits made as a result of Defendant's wrongful actions or three times Plaintiff's damages, whichever is greater;

E. Finding that this case is exceptional pursuant to 15 U.S.C. §§ 1117(a) due to Defendant's willful and intentional acts described herein and, accordingly, award Plaintiff its reasonable attorneys' fees;

F. Finding that Plaintiff is entitled to recover its costs of Court;

G. Finding that Plaintiff is entitled to prejudgment and post-judgment interest; and

H. For such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all issues so triable.

Dated: February 26, 2020

Respectfully submitted,

By: /s/Joshua D. Martin
Joshua D. Martin
Florida Bar No. 028100
josh.martin@johnsonmartinlaw.com
JOHNSON & MARTIN, P.A.
500 W. Cypress Creek Rd., Suite 430
Fort Lauderdale, Florida 33309
Telephone: (954) 790-6699
Facsimile: (954) 206-0017

Attorney for Plaintiff, TocMail Inc