IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KEEPER SECURITY, INC., Plaintiff, v. DAN GOODIN and ADVANCE MAGAZINE PUBLISHERS INC. d/b/a CONDÉ NAST and ARS TECHNICA, Defendants.	No. 17-cv-9117 Judge Joan Humphrey Lefkow Magistrate Judge Jeffrey Cole

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Dean D. Niro (dniro@vvnlaw.com)
Patrick F. Solon (solon@vvnlaw.com)
VITALE, VICKREY, NIRO & GASEY LLP
311 S. Wacker Drive, Suite 2470
Chicago, Illinois 60606
Tel.: (312) 236-0733
Fax: (312) 236-3137

Attorneys for Keeper Security, Inc.

INTRODUCTION

Defendants' December 15, 2017 Article (the "Article") falsely states as fact that the **password manager of Keeper Security, Inc. ("Keeper") had been allowing sites to "steal" passwords for "16 months"**, and that Keeper had incompetently **failed to find the vulnerability for 16 months:**

- "Microsoft is forcing users to install a critically flawed password manager: Win 10 version of Keeper has a 16-month old bug allowing sites to steal passwords";
- "Microsoft is forcing users to install a critically flawed password manager";
- "Win 10 Version of Keeper has 16-month-old bug allowing sites to steal passwords"

(ECF No. 1, Complaint ¶¶ 25, 30). Defendants' Article contradicts the true and well-pled facts that: (1) a December 2017 software issue was nothing more than a potential vulnerability in a December 8 release of the Keeper Browser Extension, which Keeper had resolved before Defendants' Article was published; (2) the purported bug was not 16 months old; (3) no Keeper software had any vulnerability, bug, flaw, or other issue between August 2016 and December 2017; (4) the December 2017 and August 2016 issues were not the same or similar; and (5) no Keeper software users were exposed to stolen passwords.

Defendants' motion asserts various defenses that cannot be decided in their favor on a motion to dismiss. Defendants solicited revenue-generating clicks on their Article by using, as bait, the false and defamatory statements claiming that Keeper's Password Manager product was no good and had been exposing customers to password theft for 16 months. Defendants did not report the truth that Keeper had immediately fixed a potential vulnerability in week-old software detected confidentially by a Google employee. Defendants had all of the true facts in their possession when they published the Article and chose to ignore them. Worse, when informed by

Keeper that the Article contained false statements, Defendants once again chose to ignore them. Defendants refused to retract the false statements in the interest of increasing their viewership.

FACTS

Keeper Security, Inc.

Keeper is a private Chicago company in the business of software security. Keeper has a software product called "Keeper® Password Manager & Digital Vault" for managing user passwords and other private information. It may be preinstalled on a device (such as a smartphone, tablet or computer) or it can be downloaded from an Internet site or Apple, Google, and Microsoft "App" stores. Keeper protects its users against hackers through its secure and convenient password manager. The users' passwords, logins, credit card numbers, bank accounts, and other personal information are saved in a private digital vault that is encrypted and highly protected. Keeper also provides additional components (which must be separately installed and logged into by the user) such as the Keeper Browser Extension. (Complaint ¶¶ 2-4).

The Keeper Browser Extension requires discretionary, manual installation by a user. A user can log into the preinstalled Keeper application, which directs users to install the Keeper Browser Extension as a separate application. If installed, the Keeper Browser Extension allows users to auto-fill login credentials (namely a user name and password) into websites for access while using a web browser. (Complaint ¶¶ 5-6).

Keeper has several million registered users and thousands of business customers who pay an annual subscription fee. The Keeper product has received thousands of five-star reviews on the App stores. Keeper fully expects that it will retain the users for several years. The users of Keeper's product rely on the integrity of the Keeper product and the reputation of Keeper in deciding to use the Keeper software. (Complaint ¶¶ 7-9).

Google Project Zero

Defendants' brief relies on hearsay documents in the form of posts to a Google database relating to Google's Project Zero. (ECF No. 15 at 2-3; ECF Nos. 15-1, 15-3). Those documents cannot be credited on a motion to dismiss. Keeper did not rely on the Google documents in the Complaint and does not concede the truth of any statements in the Google documents.

For background on Google Project Zero, see *https://security.googleblog.com/2014/07/announcing-project-zero.html.* Google's researchers privately explore unidentified "vulnerabilities" in software, including remote possibilities that hypothetically could be exploited by sophisticated hackers. Any "bugs" (Google's word) identified by the Google team are shared internally and with the relevant software vendor. This is done privately so that hackers cannot take advantage of the vulnerabilities. The software vendors want to receive and act on Google's information to preempt even remote possibilities for exploitation. Once a vendor resolves an issue, Google makes the relevant database entry public (e.g., ECF No. 15-1, posts for "Issue 1481").

The parties agree that Tavis Ormandy is a Google employee and Project Zero security researcher. As stated in a Keeper blog post (ECF No. 15-2), Keeper released a new update to the Keeper Browser Extension on December 8, 2017. On December 14, Mr. Ormandy identified a potential vulnerability in that update and contacted Keeper. On December 15, Keeper resolved the issue by updating the browser extension and disabling previous versions. (*Id.*). Then Google made the database posts public. (ECF No. 15-1). No Keeper users were ever exposed to a security breach. (Complaint ¶¶ 33, 40). There can be no dispute that Keeper immediately resolved the issue before the Google posts were made public on December 15. (*Id.* at ECF p. 2 bottom; ECF No. 15-2).

Defendants also submitted hearsay August 2016 Google posts made by Mr. Ormandy (ECF No. 15-3) and Keeper's own blog post (ECF No. 15-4). The August 2016 facts fall outside the

Complaint, and Keeper does not agree that the issues in the August 2016 documents are the same or similar. Defendants also cannot dispute that the August 2016 issue involved an earlier version of the Keeper Browser Extension and that issue was immediately resolved by Keeper. (ECF No. 15-3 at ECF p. 3; ECF No. 15-4).

Defendants' Defamatory Article

Defendants used the Google database immediately after it was published, and after Keeper resolved the issue, as a source for their December 15, 2017 Article on the for-profit website Ars Technica. (Complaint ¶¶ 19-29). The Article falsely states as fact that **Keeper's password manager had been allowing sites to steal passwords for 16 months**, and that Keeper had incompetently **failed to find the vulnerability for 16 months**. At least three specific statements in the Article (ECF No. 1-1) pound home this point:

- Microsoft is forcing users to install a critically flawed password manager: Win 10 version of **Keeper has a 16-month-old bug allowing sites to steal passwords.**

- **Microsoft is quietly forcing** some Windows 10 computers to install a **password manager that contains a critical vulnerability disclosed 16 months ago that allows websites to steal passwords**, a researcher said Friday.

- If an outsider can find **a 16-month-old vulnerability** so quickly and easily, it stands to reason **people inside the software company should have found it long ago.**

(ECF No. 1-1 at ECF pp. 2-3 (emphasis added) see Complaint ¶ 1, ¶ 30 nos. 1-3, 9).

The truth is alleged in the Complaint: No flaw of any kind had been present for 16 months. (Complaint ¶ 32). The Keeper blog dated December 15, 2017 establishes that the "browser extension update" had only been released on December 8, 2017, not 16 months before. (ECF No. 15-2). The potential vulnerability found by Mr. Ormandy on December 14 had been fixed within 24 hours. (*Id.*). Keeper's August 26, 2016 blog post likewise states that an earlier, different

security vulnerability identified by Mr. Ormandy had been resolved immediately. (ECF No. 15-4).

Further, Defendants' Article falsely stated that flawed Keeper software was being installed by force with Windows 10. The potential vulnerability identified and fixed in December 2017 related to the Keeper Browser Extension software, which was not bundled with Windows 10 and had to be installed separately. (Complaint ¶¶ 41-42).

To reinforce the false statements that Keeper users had been exposed to stolen passwords for 16 months, Defendants rang the alarm bell by adding a quotation from the Ormandy blog post claiming: "a complete compromise of Keeper security, **allowing any website to steal any password**." (ECF No. 1-1 at ECF p. 3, emphasis added; Complaint ¶ 30 no. 6).

The statements that Keeper software allowed sites to steal passwords are false. (Complaint ¶¶ 30, 31, 37, 38 and 39). Even during the few days between the December 8 release and December 15 fix of the browser extension update (ECF No. 15-2), the potential vulnerability did not expose any Keeper customer to stolen passwords. (Complaint ¶ 33). Hypothetical events that never occurred would have been required to present even the possibility of one malicious website stealing a password, including a malicious website set up with a specific type of malware. (*Id.* ¶ 40; ECF No. 15-2, second para.). And that is still a far cry from "allowing any website to steal any password". Nothing in the record identifies any such website or any such occurrence.

These statements had a defamatory "sting", telling consumers that Keeper is so terrible at password security software – a core part of Keeper's business – that Keeper left customers exposed to password theft for 16 months. One might expect consumers reading the Article to avoid Keeper entirely. In response, Keeper informed Defendants that its "relationship with vendors and customers" was at risk. (Complaint ¶ 35).

Defendants' first revised Article (ECF No. 1-2, Complaint ¶ 38), includes a note at the end about changes made after comment by Keeper and Microsoft. (ECF No. 1-2 at ECF p. 4). The Article continued to assert falsely that Keeper customers had been vulnerable to password theft for 16 months:

- Plugin for Win 10 version of Keeper had **bug allowing sites to steal passwords.**
- For almost two weeks, **Microsoft quietly forced** some Windows 10 computers to install a **password manager with a browser plugin that contained a critical vulnerability almost identical to one disclosed 16 months ago that allows websites to steal passwords**, a researcher said Friday.
- He said he uncovered a **flaw in the non-bundled version of the Keeper browser plugin 16 months ago that posed the same threat**.
- Fortunately, Windows 10 users wouldn't have been vulnerable **unless they opened Keeper, trusted it with their passwords, and used the browser plugin**."
- If an outsider can find **a bug similar to the 16-month-old vulnerability** so quickly and easily, it stands to reason **people inside the software company should have found it long ago.**

(ECF No. 1-2 at ECF pp. 2-3, emphasis added; see Complaint ¶ 38). The revised Article reported, without adopting, statements attributed to Keeper that there were two different issues 16 months apart. (ECF No. 1-2 at ECF p. 3). Defendants also added a time qualification regarding Microsoft bundling Keeper with Windows 10: "For almost two weeks, Microsoft quietly forced . . ." (*Id.*). However, the revised Article does not concede that any flaw in the Keeper software had only been present for eight days at most.

The third version of the Article continues the false statements about a long-term bug in Keeper software:

- Plugin for Win 10 version of Keeper had **bug allowing sites to steal passwords.**

- For about eight days, some versions of **Windows 10 quietly bundled** a **password manager that contained a critical vulnerability in its browser plugin**, a researcher said Friday.

- **The flaw was almost identical to one the same researcher disclosed in the same manager plugin 16 months ago that allowed websites to steal passwords**.

- He said he uncovered a **flaw in the non-bundled version of the Keeper browser plugin 16 months ago that posed the same threat**.

- Fortunately, Windows 10 users wouldn't have been vulnerable **unless they opened Keeper, trusted it with their passwords, and followed prompts to install the browser plugin**."

- If an outsider can find **a bug similar to the 16-month-old vulnerability** so quickly and easily, it stands to reason **people inside the software company should have found it first.**

(ECF No. 1-3 at ECF pp. 2-3 (emphasis added) see Complaint ¶ 39). The revision changed "two weeks" to "8 days" in the reference to Windows bundling. (See also ECF No. 1-3 at ECF p. 3 bottom (describing edit)).

As stated in the Complaint, Defendants knew the Article contained false statements and failed to speak with Keeper or verify any of the statements in the Article before its initial publication. (Complaint ¶¶ 31, 42). Defendants' revisions changed some details in the Article, while leaving the defamatory false statements about Keeper and its product. All versions continued to quote from the Ormandy blog, adding to the defamatory sting: "this is a complete compromise of Keeper security, **allowing any website to steal any password**." (ECF No. 1-2 at ECF p. 3; ECF No. 1-3 at ECF pp. 2-3).

ARGUMENT

I. Legal Standard

To survive a motion to dismiss, a complaint must allege "enough facts to state a claim to relief that is plausible of its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 569 (2007). In

other words, Keeper must make a "short and plain statement of the claim" to provide sufficient facts to plausibly suggest the allegations and give fair notice to the defendant as to what the complaint is about. *Ashcroft v. Iqbal*, 556 U.S. 662, 677 (2009). When ruling on a motion to dismiss, courts must accept all well-pleaded factual allegations as true and construe all reasonable inferences in favor of the plaintiff. *Id.*

II. Keeper Has A Claim for Defamation *Per Se*

Keeper states a claim for defamation *per se* by alleging that Defendants published injurious, false statements of fact, which can only be interpreted as telling the public that Keeper was incompetent at its business. *Solaia Tech. LLC v. Specialty Pub. Co.*, 221 Ill.2d 558, 579-80, 852 N.E.2d 825, 839 (2006) (elements); *Tuite v. Corbett*, 224 Ill.2d 490, 501, 866 N.E.2d 114, 121 (2006) (same); *Trudeau v. ConsumerAffairs.com, Inc.*, 2011 U.S. Dist. LEXIS 99852, *22, 2011 WL 3898041 (N.D. Ill. Sept. 6, 2011) (Lefkow, J.) (same).

A. The Article Is Not Substantially True

Defendants argue the substantial truth defense (ECF No. 15, pp. 6-9), which forgives erroneous details if the gist or sting of the Article is true. "The substantial truth of a statement is normally a jury question, but where no reasonable jury could find that substantial truth had not been established, the question is one of law." *Harrison v. Chicago Sun-Times, Inc.*, 341 Ill.App.3d 555, 563, 793 N.E.2d 760, 766 (1st Dist. 2003); *Trudeau*, 2011 U.S. Dist. LEXIS 99852, *23, 2011 WL 3898041. Here, the substantial truth defense cannot be decided as a matter of law.

Defendants do not argue substantial truth of the actual statements that form the "gist or sting". Defendants' Article falsely states that a security vulnerability had been present for "16 months" and that Keeper failed to find it, allowing websites to "steal" passwords from Keeper customers. The Article also falsely states that the flawed software was installed with Windows

10. (ECF No. 15-1). Defendants cannot establish substantial truth of these statements as a matter of law. The "highlight of the article, the pertinent angle of it" is false. *Trudeau,* 2011 U.S. Dist. LEXIS 99852, *23, 2011 WL 3898041 (quoting *Vachet v. Central News., Inc.*, 816 F.2d 313, 316 (7th Cir. 1987)).

Defendants are left to argue the substantial truth of a different take on the Article – that Keeper fixed a security vulnerability and the "same (or virtually identical) kind of flaw" had occurred 16 months earlier. (ECF No. 15 at 7). First, Defendants cannot argue substantial truth by recasting the Article inaccurately in their favor. Second, Defendants' version of the Article still is not substantially true. For example, Defendants' only basis for contending that the two issues were the "same (or virtually identical)" is the hearsay Google posts used as sources. The hearsay posts cannot be assumed to be true on a motion to dismiss, and Keeper disputes Defendants' version of the facts.

Defendants also rely on Keeper's own statements on a blog post. (ECF Nos. 15-2). *See Harrison*, 341 Ill.App.3d at 563, 793 N.E.2d at 766 ("Where the plaintiff's own characterization is not substantially different from the allegedly defamatory language, such language may be deemed substantially true."). Keeper's statements confirm that the Article is not substantially true. The Keeper blog dated December 15, 2017 establishes that the "browser extension update" at issue had only been released on December 8, 2017, not 16 months before. (ECF No. 15-2 at ECF p. 2 first para.). The potential vulnerability found by Mr. Ormandy on December 14 had been fixed within 24 hours. (*Id.* at third para.). The potential vulnerability required interaction with a hypothetical, malicious website that has never been identified. (*Id.* at second para.). No customer was affected. (*Id.* at sixth para.). The issue existed in a browser extension update, not software bundled with Windows 10. (*Id.* at fifth para.). Keeper's August 26, 2016 blog post also does not support

Defendants. It states that the August 2016 issue had been resolved immediately. (ECF No. 15-4). Defendants chose to ignore these facts and instead made unsupported statements.

Defendants improperly rely on Google's online posts to defend the false "16 month" statements. (ECF No. 15 at 9; ECF Nos. 15-1, 15-3). Keeper does not concede the truth of any statements in that hearsay, and facts cannot be decided adverse to Keeper on a motion to dismiss. Further, the sources lend no support to the statement that Keeper software had been vulnerable for 16 months. The December 14, 2017 post by Mr. Ormandy says he "recently created" a new Windows 10 virtual machine that included Keeper's password manager. (ECF No. 15-1 at ECF p. 2 top). He then refers to "filing a bug a while ago" and asserts "they're doing the same thing again with this version." Mr. Ormandy's earlier post in August 2016 states clearly that the problem he found on August 26, 2016 (ECF No. 15-3 at ECF p. 2) had been fixed by August 28, 2016. (*Id.* at ECF p. 3). Further, Mr. Ormandy's view of the similarity of two issues is not controlling on a motion to dismiss.

Defendants cite various substantial truth cases, none of which control here. This is not a case disputing whether a given term fits undisputed facts. Nor is it a dispute about secondary, inoffensive, or immaterial details. *Trudeau*, 2011 U.S. Dist. LEXIS 99852, *23, 2011 WL 3898041. For example, in *American Int'l Hosp. v. Chicago Tribune Co.*, 136 Ill.App.3d 1019, 1023, 483 N.E.2d 965, 969 (1st Dist. 1985), the plaintiff's own characterization of an action to "revoke" plaintiff's accreditation or "not to accredit" the plaintiff was not substantially different from a newspaper statement that the plaintiff was "refused accreditation". In *Harrison*, the *Sun-Times* used the term "kidnapped" to report a district court's judgment that the plaintiff violated a child-abduction treaty by wrongfully removing her daughter from Italy. 341 Ill.App.3d at 559-60, 793 N.E.2d at 764. After analyzing the applicable law and finding the terms "kidnapping" and "abduction" synonymous, 341 Ill.App.3d at 563-69, 793 N.E.2d at 766-71, the court held that the

term "kidnapped" conveyed the gist or sting of the legal judgment against the plaintiff. 793 N.E.2d at 771, 341 Ill.App.3d at 569. In *Vachet*, the incorrect use of the word "warrant" to describe the plaintiff's undisputed arrest for harboring a fugitive was substantially true. 816 F.2d at 316. *Wesbrook v. Ulrich*, 840 F.3d 388, 396-97 (7th Cir. 2016), which applied the truth privilege to a tortious interference claim, held that "coercion and intimidation" fairly described intimidating tactics, and "filed" fairly described oral complaints.[1] Here, terms such as "steal passwords" and "16-month-old bug" are not close to being substantially true.

B. The False Statements Have No Reasonable Innocent Construction

Defendants also rely on the Illinois innocent construction rule, which provides that some statements cannot be defamatory *per se*. More specifically, a "statement is to be considered in context, with the words and the implications therefrom given their natural and ordinary meaning; if, as so construed, the statement may reasonably be innocently interpreted or reasonably be interpreted as referring to someone other than the plaintiff it cannot be actionable *per se*." *Chapski v. Copley Press*, 92 Ill.2d 344, 352, 442 N.E.2d 195, 199 (1982).

Again, Defendants look for lower hurdles by ignoring the false statements in the Article. The Article's false statements, in context, permit only one, false, interpretation: *Keeper had left its customers exposed to password theft for 16 months.* (Complaint ¶ 30; ECF No. 1-1 at ECF pp. 2-3: "Keeper has 16-month-old bug allowing sites to steal passwords"; "password manager that contains a critical vulnerability disclosed 16 months ago that allows websites to steal passwords";

[1] Defendants cite a case that applied an "incremental harm" version of substantial truth. *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222, 1228 (7th Cir. 1993); *see Trudeau*, 2011 U.S. Dist. LEXIS 99852, *26-*28, 2011 WL 3898041 (discussing incremental harm). Defendants do not argue the incremental harm version of the defense, and this Court has noted that an Illinois appellate court declined to adopt it. *Id.* at *27.

and "people inside the software company should have found it long ago"). There is no reasonable interpretation of these statements that is innocent. No reader could conclude the "bug" was one week old when fixed and never allowed sites to steal passwords.

The statements Defendants do address fail to support dismissal under the innocent construction rule. For example, Defendants argue that the Article does not say computers are "infected", referring to Paragraph 32 of the Complaint. (ECF No. 15 at 10). The Article states: "Microsoft is quietly forcing some Windows 10 computers to install a password manager that contains a critical vulnerability disclosed 16 months ago that allows websites to steal passwords . . ." (ECF No. 1-1 at ECF p. 2). Defendants are saying that Windows 10 computers automatically have the Keeper "bug". That statement, in the context of the Article claiming that Keeper software had a bug for 16 months, is not innocent. Defendants point to the additional statement: "Fortunately, Windows 10 users aren't vulnerable unless they open Keeper and begin trusting it with their passwords." (ECF No. 15 at 10; ECF No. 1-1 at ECF p. 3). That statement, in context, is Defendants' proclamation to Windows 10 users who use the Keeper product that they are "allowing any website to steal any password". (ECF No. 1-1 at ECF p. 3). It is not innocent.

Defendants also argue that the word "vulnerability" has an innocent construction. (ECF No. 15 at 11). Not in the context of the Article, which expressly and falsely asserts a "critical vulnerability **disclosed 16 months ago that allows websites to steal passwords** . . ." (ECF No. 1-1 at ECF p. 2). Defendants are saying that the "bug" had been exposing users to password theft for 16 months. There is no innocent construction of the false accusation contained in the Article.

C. Keeper Is Not Asserting Defamation of Microsoft

Further relying on the innocent construction rule, Defendants argue that "most" of the false statements are about Microsoft, not Keeper. (ECF No. 15 at 12). Keeper has already detailed the false statements that clearly identify and defame Keeper as the source of the password manager

software. No other interpretation is plausible. Statements quoted in the Complaint that also refer to Microsoft do not support an innocent construction defense. (Complaint ¶ 30 nos. 1, 3). Other statements chide Microsoft for letting Keeper through its security vetting process. (Complaint ¶ 30 nos. 8, 10-11). The latter statements do not have to be independently actionable by Keeper. Rather, they add to the defamatory sting, by asserting that Microsoft should not be bundling Keeper with Windows 10.

D. The Defamation Is Not Opinion

Defendants argue that some words quoted in the Complaint are opinions that are not actionable. (ECF No. 15 at 13). As demonstrated above, the statements are not opinions. Further, "a false assertion of fact can be defamatory even when couched within apparent opinion or rhetorical hyperbole." *Solaia*, 221 Ill.2d at 581, 852 N.E.2d at 840. For example, Defendants described the Keeper software as "critically flawed" because "Keeper has 16-month-old bug allowing sites to steal passwords." (ECF No. 1-1 at ECF p. 2). And in fact, Defendants knew the "bug" had already been fixed. (ECF No. 15-1 at ECF p. 2, bottom). The statements are defamatory. Further, Defendants' arguments that they gave opinions about Microsoft cannot detract from the false statements of fact supporting the Keeper defamation claim, already addressed above. In any event, Keeper has a claim for defamation independent of any arguable "opinion" words used in the Article.

E. Actual Malice Is Not Required, But Is Supported

Keeper's Complaint does not support a conclusion that Keeper is a public figure, so Keeper does not have to prove actual malice. *Imperial Apparel, Ltd. v. Cosmo's Designer Direct, Inc.*, 227 Ill.2d 381, 395, 882 N.E.2d 1011, 1020 (2008). Being in business does not make Keeper a general or limited-purpose public figure. *Id.*, 227 Ill.2d at 396, 882 N.E.2d at 1021. The facts here

do not establish Keeper's general fame or its voluntary injection into a public controversy or matter of public concern, so Keeper is not a public figure. *Kessler v. Zekman*, 250 Ill.App.3d 172, 179-80, 620 N.E.2d 1249, 1254 (1st Dist. 1993). In *Kessler*, the plaintiff conceded status as a limited-purpose public figure. 250 Ill.App.3d at 181, 620 N.E.2d at 1255. The disputed broadcasts involved plaintiff's status as "the most renowned practitioner of a hotly-debated procedure". 250 Ill.App.3d at 183, 620 N.E.2d at 1256. In *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 U.S. Dist. LEXIS 20845, *12, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004), the court before trial rejected an assertion that the plaintiff's "mere status as a satellite provider" made it a public figure, but held that the plaintiff had "sufficiently interjected its position on the controversy into the public realm" to qualify. Neither is the case here.

If actual malice is determined to be a required element of the claim, Keeper's Complaint supports a plausible claim of actual malice. *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 614 (7th Cir. 2013) ("States of mind may be pleaded generally, but a plaintiff still must point to details sufficient to render a claim plausible."). Defendants' knowledge of falsity is more than plausible. All of Defendants' claimed sources are attached to their brief. Viewed in Keeper's favor on a motion to dismiss, the sources do not support the false claim of a flaw in Keeper software for 16 months, do not support the false claim that Keeper failed to find a flaw for 16 months, and do not support the false claim that Keeper's password manager allowed websites to steal passwords for 16 months. In other words, Defendants knew their statements were false.

III. Keeper States Claims for Common-Law and Statutory Trade Disparagement

Defendants apply their defamation arguments to the trade disparagement claims, and Keepers' responses apply equally. Defendants further seek to dismiss the claims for commercial disparagement and violation of the Illinois Deceptive Trade Practices Act, 815 ILCS § 510/2 on the basis that such claims are limited to "commercial speech." (ECF No. 15 at 15). The Article

definitely contains commercial speech. In order to state a commercial disparagement claim, Keeper must suggest that Defendants' "statements disparage[d]…the quality of [the Plaintiffs] goods or services." *Daniels Sharpsmart, Inc. v. Becton, Dickinson & Co.*, 2016 U.S. Dist. LEXIS 34964, *5 (N.D. Ill. March 18, 2016) (citing *World Kitchen, LLC v. The American Ceramic Society*, 2015 U.S. Dist. LEXIS 123166 (N.D. Ill. 2015) (relevant considerations include "whether:…(2) the speech refers to a specific product…"). Here, the Complaint states that "[a]ll versions of the Article falsely criticize the quality of Keeper's products and services." (Complaint ¶¶ 59-60). The Article identifies the "Keeper password manager" product. That is more than sufficient to allege commercial disparagement and a violation of the Uniform Deceptive Trade Practices Act. See *Daniels Sharpsmart, Inc.*, 2016 U.S. Dist. LEXIS at *7, ("[Plaintiff] has alleged sufficient facts relating to [Defendant's] alleged disparagement" where the statements disparage the quality of the product); *Hypergraphics Press, Inc. v. Cengage Learning, Inc.*, 2009 U.S. Dist. LEXIS 29802, *4 (N.D. Ill 2009) ("[s]tatements are not actionable under part (8) of the Uniform Deceptive Trade Practices Act unless they disparage the quality of the plaintiff's goods").

Contrary to Defendants' assertion, injunctive relief is not moot. Keeper is seeking to enjoin defendants from further using and promoting the Article in any future publication. See *Daniels Sharpsmart, Inc.*, 2016 U.S. Dist. LEXIS at *7.

CONCLUSION

Keeper respectfully requests that the Court deny the motion to dismiss. (ECF No. 14).

Respectfully submitted,
/s/ Dean D. Niro
Dean D. Niro (dniro@vvnlaw.com)
Patrick F. Solon (solon@vvnlaw.com)
VITALE, VICKREY, NIRO & GASEY LLP
311 S. Wacker Drive, Suite 2470
Chicago, Illinois 60606
Tel.: (312) 236-0733
Attorneys for Keeper Security, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on March 7, 2018 the foregoing

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

was filed electronically with the Clerk of the Court for the Northern District of Illinois using the Court's Electronic Case Filing System, which will send notification to the registered participants of the ECF System as listed:

Natalie J. Spears
Gregory R. Naron
Jacqueline A. Giannini
DENTONS US LLP
233 S. Wacker Drive, Suite 5900
Chicago, Illinois 60606
(312) 876-8000
Natalie.spears@dentons.com
Gregory.naron@dentons.com
Jacqui.giannini@dentons.com
Counsel for Defendants Dan Goodin and Advance Magazine Publishers Inc.

I certify that all parties in this case are represented by counsel who are CM/ECF participants.

/s/ Dean D. Niro
Attorneys for Keeper Security, Inc.