UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MONTGOMERY BEYER, et al., Plaintiffs, v. SYMANTEC CORPORATION, Defendant.	Case No. 18-cv-02006-EMC **ORDER GRANTING DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT** Docket No. 61

Plaintiffs Montgomery Beyer and Linda Cheslow ("Plaintiffs") bring this putative class action alleging that certain network security software products sold by Defendant Symantec Corporation ("Symantec") contained critical defects. The original complaint asserted five causes of action: (i) a California Consumer Legal Remedies Act ("CLRA") claim, (ii) a California Song-Beverly Consumer Warranty Act ("SBA") claim, (iii) a California False Advertising Law ("FAL") claim, (iv) a California Unfair Competition Law ("UCL") claim, and (v) a claim for "Quasi-Contract/Unjust Enrichment." In May 2018, Symantec moved to dismiss the original complaint. Docket No. 17. The Court granted in part and denied in part the motion. Docket No. 39. Plaintiffs then filed the operative First Amended Complaint ("FAC") on November 26, 2018. Docket No. 52. Symantec has again moved to dismiss all of Plaintiffs' claims. Docket No. 61 ("Mot.").

For the reasons discussed below, the Court finds that Plaintiffs' allegations fail to establish standing and **GRANTS** the motion to dismiss.

I. FACTUAL AND PROCEDURAL BACKGROUND

The Court's Order on Symantec's first motion to dismiss laid out the factual background of this case, which is briefly summarized here. Symantec produces and sells network security software to consumers under the Norton brand ("Norton Products") and to businesses under the Symantec brand ("Enterprise Products," and together with the Norton Products, the "Affected Products"). Docket No. 39 at 1. On April 28, 2016, a Google cybersecurity team notified Symantec of alleged vulnerabilities in the AntiVirus Decomposer Engine, a key component in the Affected Products. *Id.* at 2. In particular, the Google team discovered that the AntiVirus Decomposer Engine was defectively designed to have unrestricted access to and writing permissions for the computer's files, opening the operating system up to corruption ("High Privilege Defect"). *Id.* at 2–3. The High Privilege Defect allegedly violates the cybersecurity best practice of "the principle of least privilege," which dictates that software should operate using the least amount of privilege necessary to complete its task. *Id.* at 3. Additionally, the AntiVirus Decomposer Engine contains third party open source code that Symantec failed to update for at least seven years, resulting in critical vulnerabilities ("Outdated Source Code Defect"). *Id.*

Montgomery Beyer was the only named plaintiff in the original complaint. The FAC adds Linda Cheslow as a second named plaintiff. FAC ¶ 11. Beyer alleges he purchased five Norton Products containing the above defects. *See id.* ¶¶ 21–24. He seeks recovery for the second and third purchases only. *See id.* ¶ 21 n.12, ¶ 24 n.21. Beyer made his second purchase in March 2009, when he bought Norton 360 Premier, v. 2.0 ("Beyer Second Software") from Symantec's website. *Id.* ¶ 22. The same year, he purchased another Norton 360 Premier, v. 2.0 subscription from Best Buy ("Beyer Third Software"). *Id.* ¶ 23. Cheslow alleges she purchased two Norton Products containing the defects, and seeks recovery for both. She made her first purchase in June 2009, when she bought Norton Internet Security ("Cheslow First Software") from Symantec's website. *Id.* ¶ 25. She made her second purchase, of Norton 350 Premier, v. 4.0, in December 2010, also from Symantec's website. *Id.* ¶ 26.

Symantec and the Google team reported the Affected Products' vulnerabilities to the public on June 28, 2016, and simultaneously issued a security advisory describing software patches Symantec was deploying to resolve the vulnerabilities. FAC ¶ 4.

Symantec's first motion to dismiss contended that Beyer's original complaint failed to establish Article III standing as to the Enterprise Products under Federal Rule of Civil Procedure

12(b)(1), failed to plead the facts and circumstances of Symantec's alleged fraud regarding its software defects with the particularity required by Federal Rule of Civil Procedure 9(b), and failed to state a claim under Federal Rule of Civil Procedure 12(b)(6). *See* Docket No. 17. The Court held that Beyer had "alleged sufficient similarity between the enterprise and consumer products" to establish standing for claims based on defects in the Enterprise Products, even though he had never purchased an Enterprise Product himself. Docket No. 39 at 6. The Court dismissed claims regarding Beyer's Third Software purchase without prejudice because they were based on alleged misrepresentations on Best Buy's website, rather than statements attributable to Symantec. *Id.* at 8. The claims regarding the Beyer Second Software, on the other hand, were allowed to proceed because Symantec's statement that the software is "industry leading" may have been actionable non-puffery, and omitted mention of defects that Symantec had a duty to disclose. *Id.* at 11–15. The Court further held that Beyer had adequately alleged reliance on Symantec's misrepresentations and Symantec's knowledge of the defects at the time of sale under Rule 9(b). *Id.* at 15–17. Finally, the Court dismissed Beyer's SBA claim without prejudice because he failed to allege that the Beyer Second Software was sold at retail in California. *Id.* at 18.

The instant motion seeks dismissal of the FAC on six grounds, different from those raised in the first motion to dismiss. In particular:

(1) Plaintiffs lack Article III standing to bring any of their claims because they have not suffered a concrete and actual injury as a result of the alleged software vulnerabilities;

(2) Plaintiffs' CLRA, FAL, and UCL claims fail to plead with the particularity required by Rule 9(b) any actionable, non-puffing Symantec misrepresentation upon which Plaintiffs relied;

(3) the alleged vulnerabilities were not physical defects that were central to the functioning of the Affected Products, and therefore did not give rise to a duty to disclose the vulnerabilities;

(4) Plaintiffs have not alleged in their SBA claim that the Affected Products were unmerchantable, or that they purchased the software in California;

(5) Plaintiffs' UCL claims fail because they cannot establish any fraudulent, unlawful, or

unfair conduct on the part of Symantec; and

(6) Plaintiffs' unjust enrichment claim is duplicative of and falls with their other claims. *See* Mot. at 1–2.

II. DISCUSSION

The Court begins by addressing the "jurisdictional question of standing," which "precedes . . . analysis of the merits." *Equity Lifestyle Props., Inc. v. Cnty. of San Luis Obispo*, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008). To satisfy Article III's standing requirement, a plaintiff must demonstrate that he or she has suffered an injury in fact, that the injury is traceable to the defendant's conduct, and that the injury can be redressed by a favorable decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). The party asserting federal jurisdiction bears the burden of establishing these requirements at every stage of the litigation. *Id.* at 561. The dispute here concerns whether Plaintiffs have established injury in fact, which requires a showing that they suffered an invasion of a legally protected interest that is concrete, particularized, and actual or imminent, not merely conjectural or hypothetical. *Id.* at 560.

Based on the allegations in the FAC, Plaintiffs invoke two theories of injury. The first is the overpayment theory, whereby "a consumer alleges that he or she would not have purchased [the product], or would have paid less for it, had the seller not misrepresented the [product] or failed to disclose its limitations." *In re Chrysler-Dodge-Jeep Ecodiesel Mktg., Sales Practices, & Prod. Liab. Litig.*, 295 F. Supp. 3d 927, 945 (N.D. Cal. 2018) (hereinafter *Ecodiesel*) (citing *Hinojos v. Kohl's Corp.*, 718 F.3d 1098 (9th Cir. 2013)). The second is a theory of actual harm—for example, that the alleged defects in the Affected Products caused Plaintiffs' computer systems to be infiltrated—or, absent actual harm, a "threatened injury [that is] certainly impending." *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990).

A. Injury in Fact Based on Overpayment

Plaintiffs in their pleadings and briefing rely on the overpayment theory. They assert that "but for Symantec's material misrepresentations and omissions, which obscured critical limitations in Symantec's software, Plaintiffs would not have purchased a single Norton Product or would have paid substantially less." Docket No. 63 ("Opp.") at 7. Symantec argues such an

United States District Court
Northern District of California

assertion on its own is not enough, because the alleged vulnerabilities in the Affected Products have not caused any malfunctioning in their computer systems. Indeed, not only have the named Plaintiffs failed to allege any actual hacking or other harm; Plaintiffs fail to allege any instance of such harm has occurred to any user. Mot. at 8. According to Symantec, standing cannot be supported by a conclusory allegation of overpayment. *See id.* at 9.

The most recent and salient authority on this point is *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015). In *Cahen*, the plaintiffs alleged that the defendant motor companies equipped their vehicles with computer technology that is susceptible to third-party hacking. *Id.* at 958. But they did "not allege that any of their vehicles have actually been hacked, or that they are aware of any vehicles that have been hacked." *Id.* at 959. They pleaded the same overpayment theory of injury as Plaintiffs here, asserting that "they would not have purchased their [vehicles] or would not have paid as much as they did to purchase them" had they known that the defendants were misrepresenting the security of the technology. *Id.* at 966 (alteration in original). The district court ruled that the plaintiffs failed to establish standing, because the "entire threat [alleged] rests on the speculative premise that a sophisticated third party cybercriminal may one day successfully hack one of plaintiffs' vehicles." *Id.* This "theory of *future* injury [was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending,'" *id.* (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 401 (2013)) (emphasis and alteration in original), and failed to identify a risk of harm that was "concrete and particularized as to [the plaintiffs]," *id.* at 967 (quoting *Birdsong v. Apple, Inc.*, 590 F.3d 955, 960 (9th Cir. 2009)). The court concluded that "[w]hen economic loss is predicated solely on how a product functions, and the product has not malfunctioned, . . . something more is required than simply alleging an overpayment for a 'defective' product." *Id.* at 970 (quoting *In re Toyota Motor Corp. Unintended Acceleration Litig.*, 790 F. Supp. 2d 1152, 1166 n.11 (C.D. Cal. 2011)).

The Ninth Circuit agreed and affirmed in an unpublished order. *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720 (9th Cir. 2017). It reiterated that the alleged risks arising from the alleged vulnerability were "speculative," and had never manifested. *Id.* at 723. The plaintiffs did not, "for example, allege[] a demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values," nor "allege[] a risk so immediate that they were forced to replace or discontinue using their vehicles, thus incurring out-of-pocket damages." *Id.* Accordingly, they "failed to sufficiently allege an injury due to overpaying for their vehicles." *Id.*

Although the Ninth Circuit's decision in *Cahen* is unpublished and non-precedential, the facts closely parallel those here, and the Court finds the analysis persuasive. The alleged product defect in this case is a software vulnerability that, in theory, is susceptible to infiltration and infection. But Plaintiffs have not "allege[d] that any of their [computers] have actually been hacked, or that they are aware of any [computers] that have been hacked" as a result of the vulnerability. *Cahen*, 147 F. Supp. 3d at 959. The best they can muster is two examples of computer problems: Beyer's "computer failed to restart" after he installed the Beyer Fifth Software and there was a subsequent "considerable slowdown of his operating system." FAC ¶ 24. Unspecified "users of the Affected Products" reported on Symantec's online forums "a host of problems with their computer systems," including "severe slowdowns and degradation of computer performance, rootkits, and other types of infections related to malware and viruses," *id.* ¶ 39. Plaintiffs fail to allege a harm any more concrete than in *Cahen*. Beyer has explicitly stated that he is not pursuing a claim based on the Beyer Fifth Software, for which he received a full refund. *See id.* ¶ 24 & n.21. Nor does he link the performance problems with his computer with the Beyer Second Software or Third Software, which are the basis of his claims. And Named Plaintiffs do not suggest that they themselves experienced any of the problems reported on Symantec's forums, or that the reported problems have any causal connection with the High Privilege or Outdated Source Code Defects they complain of. *See Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 846 (N.D. Cal. 2012) ("In the class action context, the named plaintiff must show that she personally has suffered an injury, not just that other members of the putative class suffered the injury.") (citing *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022 (9th Cir. 2003)). Nor is there any evidence that the design defects alleged in this suit caused the problems reported in the online forum.

In the absence of a product malfunction, all that Plaintiffs can offer is what was found inadequate in *Cahen*—a bare assertion that they overpaid for the Affected Products. But they do not allege that disclosure of the alleged defects had "a demonstrable effect on the market" for the Affected Products, or that the vulnerabilities were such that "they were forced to replace or discontinue using their [software]." *Cahen*, 717 F. App'x at 723. If anything, Plaintiffs' case here is even more tenuous. The *Cahen* plaintiffs could at least point to the fact that the vulnerabilities in their vehicles had not yet been remedied, such that it was "'just a question of when' until hackers start infiltrating" the vehicles. 147 F. Supp. 3d at 967. In contrast, Plaintiffs' claims here rest on a purported *past* risk of harm that has never been alleged to manifest and presumably never will, given that the vulnerabilities were patched in 2016–17 and Plaintiffs had stopped using the software long before that. "[A]n economic injury that rests on the risk presented by an underlying product defect fails to establish injury in fact if the underlying risk is itself speculative." *Id.* at 970. The risk Plaintiffs cite have never materialized. Thus, Plaintiffs' "economic loss theory is not credible, as the allegations that the [Affected Products] are worth less are conclusory and unsupported by any facts." *Cahen*, 717 F. App'x at 724.

Plaintiffs argue that the "something more" requirement does not apply to them, because they are not relying on a "market effect" theory of economic loss, *i.e.*, the theory that the alleged product defect caused the market value of the product to fall. Opp. at 9. For this proposition, Plaintiffs cite *In re LinkedIn User Privacy Litigation*, No. 5:12-CV-03088-EJD, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014), which suggested that the "something more" requirement is limited to "those plaintiffs who [are] seeking to establish an economic loss based on a 'market effect' theory." *Id.* at *5. But no other case reads such a limitation into the doctrine, and Plaintiffs' reliance on *LinkedIn* is undermined by the subsequent decision in *Cahen*, where the court found that the plaintiffs failed to establish standing on either an overpayment or a market effect theory of economic loss. *See Cahen*, 147 F. Supp. 3d at 966–68, 970.[1]

[1] Plaintiffs also argue that they would not be able to invoke the market effect theory even if they wanted to, because "there is no comparable resale market that would have provided a basis for measuring a loss in market value" of their antivirus software. Opp. at 10. They point to *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Prod. Liab. Litig.*, No. MDL 2672 CRB (JSC), 2018 WL 4777134 (N.D. Cal. Oct. 3, 2018), where the court remarked that plaintiffs who leased cars that the defendants equipped with emissions cheating software could not have resold

The other overpayment cases Plaintiffs cite only underscore the deficiencies in their own complaint. *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840 (N.D. Cal. 2012) involved allegations that Apple's online App Store contained security flaws that allowed third-party software applications to upload user information from their mobile devices without permission. *Id.* at 844. The court held that the plaintiff did not have standing, because she did "not allege[] that a third-party App developer actually misappropriated her personal information, only that her personal information is at a greater risk of being misappropriated." *Id.* at 847. In *Papasan v. Dometic Corp.*, No. 16-CV-02117-HSG, 2017 WL 4865602 (N.D. Cal. Oct. 27, 2017), the plaintiff alleged that the defendant sold refrigerators with a "structural flaw" which "create[d] an unreasonable risk of fire and explosion," but the plaintiff had used her own refrigerator "without any apparent problem." *Id.* at *1, *6. The court dismissed her claim for lack of standing, finding that she had failed to show "she suffered tangible losses—economic, functional, or otherwise—from having purchased an allegedly defective Dometic refrigerator." *Id.* at *6.

In the two cases which found standing, the defendants' alleged misconduct caused actual, tangible harm. *See Ecodiesel*, 295 F. Supp. 3d at 950 (distinguishing *Cahen* because the "defeat devices" installed in defendants' vehicles to control emissions concealed that emissions were in fact well over the legal limit); *Maya v. Centex Corp.*, 658 F.3d 1060, 1069 (9th Cir. 2011) (finding standing where defendants' allegedly deceptive scheme for selling homes resulted in foreclosures in plaintiffs' neighborhoods and declines in the value of their homes). *Ecodiesel* and *Maya* are thus distinguishable.

In sum, Plaintiffs have not established standing based on an overpayment theory of injury.

B. Injury in Fact Based on Actual or Imminent Harm

Plaintiffs do not expressly invoke a theory of standing based on actual or future harm, but the Court addresses this issue briefly for the sake of completeness. As discussed above, Plaintiffs

cars they never owned, and concluded that it was "plausible that these Plaintiffs were injured when they paid money to lease vehicles that they otherwise would not have leased but for VW's emissions fraud." *Id.* at *11. But *Volkswagen Clean Diesel* is inapposite because there the defect actually manifested—the vehicles with the cheating software emitted pollutants "at levels up to 40 times the legal limit from the moment they were put in use." *Id.* at *4.

have not adequately alleged actual harm from the defects in their software; the performance issues arising from the Beyer Fifth Software and the vague complaints on Symantec's online forums have not been shown to be caused by the High Privilege and Outdated Source Code Defects in the software versions for which Named Plaintiffs seek recovery. But the absence of actual harm is not dispositive, because an injury supporting Article III standing can be "actual *or* imminent." *Clapper,* 568 U.S. at 409 (emphasis added) (citation omitted).

For instance, in a line of cases that is in many ways analogous to software vulnerability cases, the Ninth Circuit has held that plaintiffs whose personal information has been compromised in data breaches can establish standing without showing that their information was in fact misused. However, in these cases, the plaintiffs must allege a "credible threat" of future harm arising from the data breach that is "real and immediate." *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). In other words, "[a]lthough imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative." *Lujan*, 504 U.S. at 565 n.2 (internal quotation marks omitted). Thus, for example, courts have found standing in data breach cases, even though the plaintiffs' personal information had not yet been misused by the hackers, where the hackers spent several weeks collecting particularly sensitive personal data, and that the stolen data had already surfaced on the dark web. *In re Adobe Systems, Inc. Privacy Litigation,* 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014). These two considerations indicated that the threat of identity threat was credible, rather than merely speculative.

Such indicia are absent here. Instead, this case is similar to *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078 (E.D. Cal. 2015), a data breach case in which there were no allegations of actual misuse of the stolen data, even though "almost four years has elapsed since the Data Breach." *Id.* at 1087–88. Because years had passed since the breach without any evidence that the data had been misused, the court concluded that the plaintiff had not demonstrated "a substantial risk of imminent future harm of identity theft." *Id.* at 1088. The same conclusion obtains here. The alleged defects in the Affected Products were revealed in 2016, but despite the fact that the defect here existed since 2005, *see* FAC ¶ 1, Plaintiffs have not cited a single example of computer malfunction causally connected to the defect. The Named Plaintiffs also stopped using the Affected Products years ago.[2] Accordingly, they have not "alleged a credible threat of real and immediate harm stemming from the [alleged defects]." *Krottner*, 628 F.3d at 1143.

As Plaintiffs have failed to establish the jurisdictional requirement of Article III standing, their claims must be dismissed, and the Court need not reach Symantec's remaining arguments for dismissal. The Court, however, will allow Plaintiffs one more opportunity to amend their complaint. Plaintiffs' counsel stated at the February 14, 2019 hearing that with further investigation, they may be able to allege that the computer malfunctions Beyer experienced after installing the Beyer Fifth Software, as well as the performance issues reported on Symantec's online forums, are attributable to the High Privilege and Outdated Source Code Defects. While the Court cannot say at this point whether such allegations will be enough to establish standing as to the Named Plaintiffs, leave to amend shall be freely given when justice so requires," and amendment would not clearly be futile. *See* Fed. R. Civ. P. 15(a). To that end, the parties represented at the hearing that they could engage in limited and focused discovery: Plaintiffs will be given: (1) documents in Symantec's possession pertaining to known or suspected incidents of third-party hacking or exploitation arising from the alleged defects, and (2) relevant source code that would allow Plaintiffs to determine whether there is a causal link between the alleged defects and reported malfunctions. Such discovery shall be produced within thirty (30) days of this order. Plaintiffs shall have sixty (60) days from the order to file a Second Amended Complaint, provided it can do so consistent with Rule 11.

///

///

///

///

///

///

[2] Plaintiffs thus have no standing to seek injunctive relief. *See City of Los Angeles v. Lyons*, 461 U.S. 95, 106 (1983).

III. CONCLUSION

For the foregoing reasons, Symantec's motion to dismiss is **GRANTED** with respect to all claims. Plaintiffs shall have leave to amend their complaint within sixty (60) days.

This order disposes of Docket No. 61.

IT IS SO ORDERED.

Dated: February 26, 2019

EDWARD M. CHEN
United States District Judge

United States District Court
Northern District of California