UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
CIVIL MINUTES—GENERAL

Case No.	**CV 17-4309-DMG (Ex)**	Date	September 6, 2018
Title	***Steven J. Brett v. Brooks Bros. Grp., Inc.***	Page	1 of 7

Present: The Honorable DOLLY M. GEE, UNITED STATES DISTRICT JUDGE

KANE TIEN	NOT REPORTED
Deputy Clerk	Court Reporter
Attorneys Present for Plaintiff(s) None Present	Attorneys Present for Defendant(s) None Present

Proceedings: IN CHAMBERS - ORDER RE DEFENDANT'S MOTION TO DISMISS [33]

Before the Court is Defendant Brooks Brothers Group, Inc.'s ("Brooks Brothers") Motion to Dismiss ("MTD") [Doc. # 33] Plaintiffs Steven Brett and America Munson's Second Amended Class Action Complaint ("SAC") [Doc. # 32]. The SAC alleges causes of action for (1) breach of implied contract; (2) negligence; (3) unlawful business practices under the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq.*; (4) unfair business practices under the UCL; (5) fraudulent/deceptive business practices under the UCL; (6) breach of covenant of good faith and fair dealing; and (7) violation of California's Data Breach Act, Cal. Civ. Code § 1798 *et seq*. [Doc. # 32.] Brooks Brothers seeks dismissal under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The MTD is fully briefed [Doc. ## 33 (MTD), 34 ("Opp'n"), 36 ("Reply")], and for the reasons that follow, the Court **GRANTS** the MTD.

I.
PROCEDURAL BACKGROUND

Scott Ables first filed suit, as a putative class action, against Defendant on June 9, 2017. [Doc. # 1.] He filed a first amended complaint ("FAC") on July 13, 2017. [Doc. # 13.] On June 7, 2018, the Court granted Brooks Brothers' motion to dismiss the FAC for lack of subject matter jurisdiction and granted Ables limited leave to amend. [Doc. # 31 ("MTD Order").]

Upon filing the SAC, Plaintiffs Brett and Munson were added as named plaintiffs. [Doc. # 32.] After Defendant filed the instant MTD, Plaintiffs simultaneously filed their opposition and a notice of voluntarily dismissal of former lead plaintiff Ables' claims, effectively making Brett and Munson the only named plaintiffs. [Doc. ## 34–35.]

II.
FACTUAL BACKGROUND[1]

Brooks Brothers is a clothing retailer. *See* SAC at ¶ 1. Plaintiffs, California residents, and putative class members, residents of states across the country, are former Brooks Brothers customers who purchased merchandise at Brooks Brothers stores from April 4, 2016 to March 1, 2017. *Id.* at ¶¶ 2, 6–7, 10, 81.

On or around April 4, 2016, malware was installed on Brooks Brothers' point-of-sale ("POS") systems, affecting at least 223 Brooks Brothers locations. *Id.* at ¶ 32. Brooks Brothers allegedly failed to implement and maintain reasonable security procedures and practices, including administrative, technical, and physical safeguards, to protect customers' private identifying information ("PII"). *Id.* at ¶¶ 50, 66. Due to the data breach, an unauthorized third party collected the full names, credit and debit card numbers, expiration dates, and verification codes of Brooks Brothers' customers, and—"upon information and belief"—information about which stores and at what time the customers' Brooks Brothers' transactions took place, from approximately April 4, 2016 until March 1, 2017. *Id.* at ¶¶ 3, 32, 34.

Plaintiff Munson used one credit card and at least two other debit cards to make purchases at Brooks Brothers stores during the timeframe of the data breach. *Id.* at ¶ 6. At an unspecified time, she discovered fraudulent activity on one of those debit cards, which she later canceled. *Id.* at ¶ 6. Plaintiff Brett had also made purchases at Defendant's stores before, during, and after the duration of the data breach. *Id.* at ¶ 7. It does not appear that he ever suffered fraudulent activity in connection with any credit or debit cards used at Defendant stores.

On May 12, 2017, Brooks Brothers disclosed the data breach on its website. *Id.* at ¶ 35. The disclosure explains, *inter alia*, that the breach could affect some customers' payment card information, but that no sensitive personal information, such as social security numbers or addresses, were affected. Ex. 31 to SAC [Doc. # 32-31].

[1] The Court accepts all material facts alleged in the SAC as true solely for the purpose of deciding the MTD. Because Scott Ables voluntarily dismissed his claims against Defendant after the SAC, the Court will not take into consideration the SAC's allegations as they are particularized to him.

III.
DISCUSSION[2]

Brooks Brothers seeks dismissal of the SAC for several deficiencies. The MTD also raises the serious procedural misstep Plaintiffs have taken here with respect to the overly broad SAC and inclusion of new parties without the Court's leave. The Court first addresses the SAC's procedural defects and then turns to analyze the merits of the action.

A. Procedural Defects

It is well established in this Circuit that a district court may strike or dismiss claims or parties included in an amended pleading without the court's leave. *See, e.g.*, *Jameson Beach Prop. Owners Ass'n v. United States*, No. CV 13-01025-MCE-AC, 2014 WL 4925253, at *3–4 (E.D. Cal. Sept. 29, 2014) ("District Courts in this circuit generally allow plaintiffs to add new claims and/or parties to an amended complaint where a prior order of dismissal granted leave to amend without limitation. On the other hand, where a prior court order granted limited leave to amend, District Courts in this circuit generally strike new claims or parties contained in an amended complaint when the plaintiff did not seek leave to amend. . . . When the language of an order clearly states that a plaintiff may only amend to address certain deficiencies identified in the order, courts have held that a plaintiff is barred from adding new claims or parties." (citation omitted) (collecting cases)); *Raiser v. City of Los Angeles*, No. CV 13-2925 RGK (RZx), 2014 WL 794786, at *4 ("C.D. Cal. Feb. 26, 2014) ("When a district court grants leave to amend for a specified purpose, it does not thereafter abuse its discretion by dismissing any portions of the amended complaint that were not permitted. The rule applies even if the court did not expressly bar amendments other than the one(s) it *did* allow." (citation omitted)); *Benton v. Baker Hughes*, No. CV 12-07735 MMM (MRWx), 2013 WL 3353636, at *3 (C.D. Cal. June 30, 2013) (striking claims added in amended complaint where earlier dismissal order granted plaintiff "leave to amend only to address the deficiencies in his existing causes of action identified in [the] order").

Here, the Court granted Ables leave to amend "to cure the deficiencies identified" in the Order based on facts and arguments discussed in Ables' opposition brief that were absent from the FAC. MTD Order at 11. The Court did not grant Ables leave to substitute or add named plaintiffs, and Ables never sought leave to do so. Moreover, those facts and arguments in Ables' opposition brief that served as the basis for leave to amend are notably absent from the SAC, notwithstanding

[2] The Court incorporates by this reference the relevant legal standards that it set forth in its prior Order. *See* MTD Order at 2–4.

the fact that Ables voluntarily dismissed his claims against Defendant *after* filing the amended complaint. [Doc. ## 32 (SAC filed June 28, 2018), 34 (Opp'n filed August 3, 2018), 35 (Ables' voluntarily dismisses claims August 3, 2018).]

The Court therefore **STRIKES** Plaintiffs Munson and Brett's claims against Defendant. Because Ables has voluntarily dismissed his claims against Defendant, this effectively disposes of the entire case. In an abundance of caution, however, the Court briefly considers the merits of the motion and begins with the threshold issue of standing.

B. Article III Standing[3]

Defendant contends that Plaintiffs cannot demonstrate any of the elements of Article III standing. With respect to the injury-in-fact requirement, the parties chiefly dispute whether Plaintiffs have sufficiently alleged an imminent risk of future harm. *See* Opp'n at 12–16[4] (maintaining only one theory of injury in fact in response to the MTD). As nonmovants, Brett and Munson bear the burden of establishing standing. *See, e.g.*, *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1208 (N.D. Cal. 2014).

Plaintiffs contend that as a result of the data breach there is a credible risk of future harm from identity theft based on (1) Munson's "open and active" credit cards; and (2) the purchase information hackers likely obtained, which Plaintiffs insist permits hackers to "link" information actually obtained with other PII not obtained in order to commit identity theft. Opp'n at 13, 14–15.

Even in light of the new facts alleged, *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) and *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018)—the two leading data breach cases in this Circuit that concern standing based on an alleged risk of future identity theft—are still distinguishable and do not warrant a finding of injury-in-fact sufficient to confer Article III standing in this case. While the Court agrees with Plaintiffs that the absence of social security numbers in compromised datasets does not foreclose a finding of a credible threat of future harm, Plaintiffs' compromised data does not create the same level of imminence of a future harm as found in *Krottner* and *Zappos*. As the Court explained in the MTD Order, the hackers in *Krottner*

[3] The Court incorporates by this reference its earlier articulation of Article III standing requirements. *See* MTD Order at 4.

[4] Citations to the parties' moving papers refer to the pagination assigned by the CM/ECF docketing system.

obtained unencrypted names, addresses, and social security numbers, and the *Zappos* hackers obtained names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, full credit card numbers, and unspecified credit and debit card "information." MTD Order at 8 (citing *Zappos*, 888 F.3d at 1023; *Krottner*, 628 F.3d at 1140). Based on "the sensitivity of the personal information, combined with its theft," plaintiffs in those cases "adequately alleged an injury in fact supporting standing." *Zappos*, 88 F.3d at 1027.

Here, hackers stole Plaintiffs' names, credit and debit card numbers (along with card expiration dates and verification codes) and possibly the Brooks Brothers store zip codes where Plaintiffs made purchases as well as the time of those purchases. SAC at ¶ 32. This information simply does not rise to the level of sensitivity of the information in *Krottner* and *Zappos* or similar cases. *See Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No.: CV 16-00014-GPC-BLM, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016) ("[T]he information stolen during the Starwood breach [names, addresses, billing information, and credit card numbers] is insufficient, for example, for a third party to open up a new account in Plaintiff's name or to gain access to personal accounts likely to have the information needed to open such an account (e.g., a social security number)."); *cf.* MTD Order at 8 (collecting within-Circuit cases where the district court found an injury-in-fact based on increased risk of future harm, and enumerating the PII obtained in those cases).[5]

The added allegations involving Defendant store zip codes and purchasing times adds little to the standing analysis. Brooks Brothers' customers may make purchases within or outside of their home or employer's zip code, so the acquisition of that information does not make the risk of identity theft more likely. More importantly, based on the PII allegedly obtained in this case, Plaintiff's linking theory requires the Court to make a series of speculative inferences to conclude that Plaintiffs suffer a credible, imminent risk of identity theft. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013) ("[A] theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly

[5] The Court recognizes that in *Zappos*, the Ninth Circuit remarked on the sensitive nature of credit card numbers. Despite this, the *Zappos* Court did not signal that the disclosure of credit card numbers alone would suffice to establish an injury-in-fact based on risk of future harm. Rather, the Court opined on the combination of sufficiently sensitive PII that permitted the plaintiffs' allegations to demonstrate an injury-in-fact. Moreover, Plaintiffs here have not pointed to any authority that supports the proposition that disclosure of credit card information alone is sufficient to show a concrete, imminent risk of future harm, and this Court's independent review of the case law shows the opposite, even since *Zappos*' issuance. *See Jacobson v. Peter Piper, Inc.*, No. CV-16-0596-TUC-JAS (LCK), 2018 WL 3719324, at *3 n.3 (D. Ariz. June 28, 2018) (rejecting contention that *Zappos*' acknowledgment of credit card sensitivity amounts to a finding that disclosure of such information is sufficient to confer standing).

impending."); *Dugas* (no injury in fact based on risk of future harm where "the small amount of useful" PII obtained required the Court "to engage in a hypothetical line of reasoning in order to conclude that Plaintiff remains at risk of imminent identity theft").

Nor does the fact that Munson has closed only one debit card account after discovering fraudulent activity change the Court's standing analysis. In the MTD Order, the Court explained that then-Plaintiff Ables could not rely on the theft of his cancelled credit and debt card information to show a present or sufficiently credible future injury. *See* MTD Order at 7 (present injury), 8 (future injury). The Court had already ruled that the compromise of his credit card information and his name were insufficient to show a serious risk of future injury, and the fact that Ables had since closed his compromised accounts was a secondary consideration that supported dismissal. Furthermore, it has been over one year since hackers obtained card numbers connected with Munson's open and active accounts, which weighs against a finding of imminent future harm. *See* SAC at ¶ 32 (malware installed on or about April 4, 2016), ¶ 34 (malware acquired customer PII until around March 1, 2017); Doc. # 32 (SAC filed June 28, 2018). Plaintiffs contend that this fact cannot counsel against a finding of standing because federal jurisdiction "depends upon the state of things at the time of the action brought." Opp'n at 15 (quoting *Mollan v. Torrance*, 22 U.S. 547, 539 (1824)). Be that as it may, *these Plaintiffs* brought suit when they filed the SAC; Ables served as the sole named plaintiff until this iteration of the pleading.

Finally, Plaintiffs insist that by informing their customers to monitor their credit and debit accounts, Brooks Brothers effectively acknowledged a risk of future harm to their customers sufficient to confer standing. *See* SAC at ¶ 54; Doc. # 32-31 (copy of Defendant's message regarding the hack). Not only does such an argument rest on a misunderstanding of *Zappos*, but also it creates a perverse policy incentive.

In *Zappos*, the Court concluded that even though the data breach there did not result in hackers' acquisition of social security numbers, "the information taken in the data breach [names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, full credit card numbers, and unspecified credit and debit card "information"] still gave hackers the means to commit fraud or identity theft"—a conclusion which the company "effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used 'the same or a similar password'" as the one obtained in the breach. 888 F.3d at 1027. Plaintiffs' argument here extends *Zappos* too far. Zappos' instructions to their customers acknowledged that passwords give third parties "the means" to commit fraud or identity theft; the company's warning *qua* warning did not establish credibility of future harm. *Id.* With only credit

card numbers, names, and Brooks Brothers transaction locations and times, the threat of future harm is more conjectural than credible.[6]

Furthermore, Brooks Brothers' disclosure, including the directive about monitoring account statements, is required by law. *See* Cal. Civ. Code § 1798.82(d)(1). The Court will not interpret bare statutory compliance as an affirmative admission of imminent future harm. Indeed, such an interpretation would require courts to conclude that a data breach's mere occurrence establishes imminent risk of future harm, which is contrary to controlling Article III precedent, and it would perversely incentivize companies to provide vague or misleading disclaimers to customers affected by a data breach in an attempt to avoid litigation.

Because Plaintiffs' only theory of injury-in-fact fails to demonstrate Article III standing, the Court **GRANTS** the MTD for lack of subject-matter jurisdiction. Accordingly, the Court does not address Defendant's alternative grounds for dismissal for failure to state a claim under Rule 12(b)(6). Plaintiffs have been unable, after three complaints and three separate named complainants, to allege facts sufficient to confer standing. Amendment would thus be futile, and the Court **DENIES** any further leave to amend.

IV.
CONCLUSION

In light of the foregoing, the Court **GRANTS** the MTD, without prejudice, for lack of subject matter jurisdiction.

IT IS SO ORDERED.

[6] This same logic extends to why the Ninth Circuit adopted concepts of "phishing" and "pharming" in *Zappos*, but why those same concepts are too remote in this case. *See* 888 F.3d at 1027. The more PII a third party already possesses, the easier it is to fill in the remaining gaps. *Id.* For example, with an email address and password, an individual could reset a username and password to nearly any website, including bank websites, and gain access to documents and PII that would most certainly present a serious risk of future identity theft.