

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

MICHAL FUS, individually and on behalf)	
of all others similarly situated,)	
)	
Plaintiff,)	
)	No. 19-cv-06601
v.)	
)	Judge Andrea R. Wood
CAFEPRESS, INC.,)	
)	
Defendant.)	

MEMORANDUM OPINION AND ORDER

Plaintiff Michal Fus is a former customer of Defendant CafePress, Inc.’s (“CafePress”) online gift shop. In October 2019, CafePress notified Fus and millions of its other customers that a data security incident might have compromised their personal information. Due to CafePress’s allegedly inadequate data security practices, Fus claims that he and CafePress’s customers face an increased risk of identity theft and fraud. As a result, Fus brought the present action on behalf of himself and a class of similarly situated CafePress customers whose personal information was compromised in the data breach. Now before the Court are CafePress’s motion to dismiss pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) (Dkt. No. 17), CafePress’s motion to compel arbitration (Dkt. No. 45), and Fus’s motion to strike declarations submitted by CafePress in support of its motion to dismiss (Dkt. No. 31). For the reasons that follow, the Court denies Fus’s motion to strike, grants CafePress’s motion to dismiss for lack of subject-matter jurisdiction, and denies as moot CafePress’s motion to compel arbitration.

BACKGROUND

As alleged in the Complaint, CafePress runs an online gift shop at www.cafepress.com and ships its merchandise throughout the nation. (Compl. ¶¶ 1, 9, Dkt. No. 1.) On February 20,

2019, CafePress's online databases were hacked, exposing the data associated with a total of 23,205,290 user accounts. (*Id.* ¶ 11.) Fus alleges that the compromised data included users' email addresses, passwords, names, addresses, phone numbers, the last four digits of their credit card numbers, credit card expiration dates, and Social Security numbers. (*Id.*) Fus further alleges that CafePress did not notify its customers of the data breach until October 2, 2019, when it sent them an email about a "data security incident" involving their personal information. (*Id.* ¶¶ 2, 26.)

Fus identifies himself of one of the CafePress customers whose information was exposed as a result of the hack. (*Id.* ¶ 8.) He claims that, upon receiving the notification of data breach, he spent time and money to mitigate potential harm by employing a credit monitoring service and freezing his credit. (*Id.* ¶ 8.) In addition, Fus predicts he will spend time and effort making phone calls to his bank and credit card company, monitoring his financial accounts, searching for fraudulent activity, and reviewing his credit reports. (*Id.*) Fus claims that had he known of CafePress's inadequate data security practices, he would never have patronized its website. (*Id.*)

DISCUSSION

Fus has brought the present action on behalf of himself and a putative class of similarly situated individuals whose information was compromised in the February 2019 data breach. His Complaint sets forth claims for common law negligence and violations of various Illinois state statutes. Presently before the Court are two motions brought by CafePress and one by Fus. First, CafePress moves to dismiss the action either under Rule 12(b)(1) for lack of standing or, alternatively, under Rule 12(b)(6) for failure to state a claim. Along with his brief in response to CafePress's motion to dismiss, Fus has separately moved to strike two declarations CafePress submitted in support of its motion, arguing that those declarations constitute matters outside the pleadings that cannot be considered at the motion to dismiss stage. In addition, several months

after moving to dismiss, CafePress also filed a motion to compel arbitration, claiming that Fus entered into a written arbitration agreement with CafePress that covers all claims set forth in his Complaint.

As a threshold matter, however, the Court must address whether Fus has standing to bring this action. *See Elsassner v. DV Trading, LLC*, 444 F. Supp. 3d 916, 920 (N.D. Ill. 2020) (“Standing must be considered before reaching defendant’s motion to compel [arbitration] because the [Federal Arbitration Act, 9 U.S.C. § 1 *et seq.*] ‘bestows no federal jurisdiction but rather requires for access to a federal forum an independent jurisdictional basis over the parties’ dispute.” (quoting *Vaden v. Discovery Bank*, 556 U.S. 49, 59 (2009))); *Halperin v. Int’l Web Servs., LLC*, 70 F. Supp. 3d 893, 897 (N.D. Ill. 2014) (“Because standing is jurisdictional, the court must consider that issue before reaching the merits.”). Standing is an essential component of Article III’s limitation of federal courts’ judicial power only to cases or controversies. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). “The doctrine limits the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong.” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). There are three elements that constitute the “irreducible constitutional minimum” of standing. *Lujan*, 504 U.S. at 560. A “plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo*, 136 S. Ct. at 1547 (internal quotation marks omitted). Where a plaintiff does not have Article III standing, a federal district court lacks subject-matter jurisdiction to hear his or her claims. *Simic v. City of Chicago*, 851 F.3d 734, 738 (7th Cir. 2017).

A defendant may raise either a facial or factual challenge to a plaintiff’s standing. *Silha v. ACT, Inc.*, 807 F.3d 169, 173 (7th Cir. 2015). A facial challenge requires “only that the court look

to the complaint and see if the plaintiff has sufficiently *alleged* a basis of subject matter jurisdiction.” *Apex Digit., Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443 (7th Cir. 2009). By contrast, “a factual challenge lies where the complaint is formally sufficient but the contention is that there is *in fact* no subject matter jurisdiction.” *Id.* at 444 (internal quotation marks omitted). Where a defendant mounts a factual challenge, “the court may look beyond the pleadings and view any evidence submitted to determine if subject matter jurisdiction exists.” *Silha*, 807 F.3d at 173. Once a defendant has proffered evidence calling the plaintiff’s standing into question, “the presumption of correctness that [is] accord[ed] to a complaint’s allegations falls away . . . and the plaintiff bears the burden of coming forward with competent proof that standing exists.” *Apex Digit.*, 572 F.3d at 444 (internal quotation marks and citations omitted).

Here, CafePress mounts a factual attack to Fus’s standing by submitting declarations from Cody Martinho, a CafePress Manager of Business Technology Services (Martinho Decl., Dkt. No. 18), and Cary D. Sullivan, one of CafePress’s counsel of record in this matter (Sullivan Decl., Dkt. No. 19). In his declaration, Martinho attests that he has searched CafePress’s customer transaction database for transactions involving Fus and found records for two separate transactions: one from November 2008 and another from December 2014. (Martinho Decl. ¶ 3.) He further states that for the 2008 transaction, nearly all Fus’s personal information was permanently deleted by CafePress in 2018—*i.e.*, prior to the data breach—as part of a clean-up of old information. (*Id.* ¶ 4.) “The only information that CafePress retained relating to this transaction, following the clean-up, is [Fus’s] personal email address[,] the city/state/zip of the billing address[,] the city/state/zip of the shipping address[,] and the expiration month and year of the credit card used to make the purchase.” (*Id.*) With respect to Fus’s 2014 transaction, Martinho states that the record reflects that the purchase was billed to an individual named Julie Freydin

and shipped to Fus at his employer's address. (*Id.* ¶ 5.) Sullivan's declaration further elaborates that Fus's counsel confirmed that Fus used his employer's credit card, which was in Julie Freydin's name, to make the 2014 purchase. (Sullivan Decl. ¶ 2.)

According to CafePress, the two declarations demonstrate that Fus does not have standing to pursue this suit because the data breach did not cause him an injury-in-fact. Specifically, CafePress contends that its evidence establishes that none of Fus's non-public personal or financial information could have been exposed in the February 2019 data breach because CafePress no longer possessed such information relating to Fus at the time of the breach. To support standing, "an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l, USA*, 568 U.S. 398, 409 (2013) (internal quotation marks omitted). "Allegations of future harm can establish Article III standing if that harm is 'certainly impending,' but 'allegations of possible future injury are not sufficient.'" *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692 (7th Cir. 2015) (quoting *Clapper*, 568 U.S. at 409). In a class action, "a named plaintiff cannot acquire standing to sue by bringing his action on behalf of others who suffered injury which would have afforded them standing had they been named plaintiffs." *Payton v. County of Kane*, 308 F.3d 673, 682 (7th Cir. 2002) (internal quotation marks omitted). Put differently, a named plaintiff "cannot predicate standing on injury which he does not share." *Id.* (internal quotation marks omitted).

The Court finds that CafePress's declarations successfully call Fus's standing into question. Fus's claimed injuries all arise from the allegation that his non-public personal and financial information was obtained by criminals who may use it to steal his identity or otherwise defraud him. The Seventh Circuit has held that customers whose data is acquired in a data breach

may suffer several concrete and particularized injuries sufficient for standing. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966–69 (7th Cir. 2016); *Remijas*, 794 F.3d at 691–94. In both *Lewert* and *Remijas*, the plaintiffs alleged that hackers had deliberately targeted and obtained customers' credit and debit card information, and at least some customers had found fraudulent charges on their financial statements. *Lewert*, 819 F.3d at 965; *Remijas*, 794 F.3d at 690. Based on those allegations, the Seventh Circuit found “two future injuries that were sufficiently imminent: the increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft.” *Lewert*, 819 F.3d at 966 (citing *Remijas*, 794 F.3d at 691–94). In addition, the Seventh Circuit recognized that the mitigation expenses the plaintiffs incurred to protect against future identity theft or fraudulent charges qualified as “actual injuries” given that the data breach had already occurred, making the harm imminent. *Lewert*, 819 F.3d at 967; *Remijas*, 794 F.3d at 694.

Critical to the Seventh Circuit's finding of cognizable injuries-in-fact in both *Lewert* and *Remijas* was the fact that the plaintiffs had alleged that the data stolen was sufficiently sensitive to expose the victims to a material risk of identity theft or fraudulent transactions. *See Kylie S. v. Pearson PLC*, No. 19 C 5936, 2020 WL 4336072, at *3 (N.D. Ill. July 28, 2020) (“When the *Remijas* court analyzed the risk of identity theft, it repeatedly highlighted the sensitive nature of the compromised data and the actual incidences of fraudulent charges”); *In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) (“Unlike the data breaches in *Lewert* and *Remijas*, the data stolen here did not include credit-card or debit-card information, or any other information that could easily be used in fraudulent transactions.”). But here, CafePress's evidence shows that none of Fus's personal or financial information exposed in the February 2019 data breach was particularly sensitive. Rather, most of Fus's information

possessed by CafePress at the time of the hack was publicly available information, such as his billing and shipping address and personal email address. However, the disclosure of such information does not expose Fus to a significant risk of identity theft or fraud. *See, e.g., Jackson v. Loews Hotels, Inc.*, No. ED CV 18-827-DMG (JCx), 2019 WL 2619656, at *3–4 (C.D. Cal. Jan. 4, 2019) (finding that the plaintiff suffered no injury-in-fact when only publicly available information such as her “full name, email, phone number, and address” was exposed in data breach); *In re VTech Data Breach Litig.*, 2017 WL 2880102, at *4 (“It is unclear how the disclosure of plaintiffs’ names, addresses, birthdates, and VTech account information would increase the risk of fraudulent transactions on plaintiffs’ credit cards or fraudulent accounts being opened in their names.”).

The most sensitive information that CafePress retained related to Fus was the expiration date of his credit card used in the 2008 transaction. By itself, that information is not particularly useful to an identity thief. *Cf. Meyers v. Nicolet Rest. of De Pere, LLC*, 843 F.3d 724, 727–28 (7th Cir. 2016) (finding, in an action under the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681c(g)(1), that a defendant’s failure to truncate a credit card’s expiration date on a receipt did not create an appreciable risk of harm, and noting that “Congress has specifically declared that failure to truncate a card’s expiration date, without more, does not heighten the risk of identity theft”). While an identity thief could use Fus’s credit card expiration date to perpetrate fraud, he would need additional information, such as the credit card number and the CVV code. Such information was not compromised in the February 2019 data breach. It is theoretically possible that the same hackers could have obtained that information through other means and then paired it with the credit card expiration date they acquired in the CafePress data breach, but such a

speculative injury based on “uncertain contingencies” cannot create an injury that supports standing. *Kylie S.*, 2020 WL 4336072, at *4.

Because CafePress has called Fus’s standing into question, Fus has the burden of coming forward with evidence establishing his standing. Instead, Fus filed a motion to strike CafePress’s declarations, arguing that the facts set forth in those declarations are matters outside the pleadings used to mount a substantive defense to the merits of Fus’s claims. To support his argument, Fus cites *Craftwood II, Inc. v. Generac Power Systems, Inc.*, 920 F.3d 479 (7th Cir. 2019). There, the Seventh Circuit reversed a district court’s dismissal of claims under the Telephone Consumer Protection Act, 47 U.S.C. § 227, for lack of subject-matter jurisdiction because it found that the district court had erroneously treated “a defense as if it were an element of subject-matter jurisdiction.” *Id.* at 481. But in *Craftwood II*, the Seventh Circuit found that the plaintiffs had alleged injury from the defendants’ unsolicited faxes in the form of the cost of the paper and toner used to print the fax and the time the plaintiffs’ employees dedicated to read those faxes. *Id.* While those injuries “may have been slight,” they were nonetheless “concrete rather than abstract losses.” *Id.* Unlike in *Craftwood II*, here, Fus has not alleged that the data breach has already caused him a concrete loss; he alleges only that the hackers might use his personal or financial information sometime in the future to steal his identity or otherwise defraud him. Such allegations of future harm can constitute an injury-in-fact that confers standing but only where the allegations demonstrate that the injury “is certainly impending.” *Clapper*, 568 U.S. at 409. Thus, CafePress’s declarations go directly to the issue of the concreteness of Fus’s alleged injuries because the statements contained therein challenge the imminence of the injury he alleges.

Furthermore, Fus points to no authority suggesting that the evaluation of the imminence of an alleged future injury in the data breach context is a merits issue. To the contrary, numerous

courts both within this Circuit and outside it have evaluated the sufficiency of a plaintiff's allegations of a substantial risk of future harm from a data breach as part of an Article III standing analysis. *E.g.*, *Kylie S*, 2020 WL 4336072, at *3–5; *In re VTech Data Litig.*, 2017 WL 2880102, at *3–5; *Khan v. Child.'s Nat'l Health Sys.*, 188 F. Supp. 3d 524, 529–33 (D. Md. 2016). In short, because CafePress properly uses the two declarations to support its factual attack on standing, the Court may consider the facts contained in those declarations in connection with CafePress's Rule 12(b)(1) motion. Fus's motion to strike the declarations is thus denied.

Because Fus fails to come forward with his own evidence to support his standing, CafePress's declarations are unrebutted. And those declarations establish that Fus sustained no injury-in-fact from the February 2019 data breach because he does not face a substantial risk of future harm from exposure of the non-sensitive personal and financial information CafePress possessed related to him. While Fus also alleges that he expended time and money to protect himself from identity theft and fraud after receiving notification of the data breach, such "mitigation expenses qualify as 'actual injuries' only when the harm is imminent." *Lewert*, 819 F.3d at 967; *see also In re VTech Data Litig.*, 2017 WL 2880102, at *5 ("[W]ithout imminent harm, mitigation expenses do not meet the injury-in-fact requirement . . ."). Given that Fus faces no imminent harm from the data breach, he cannot predicate an injury-in-fact on his mitigation expenses even though they have already been incurred in response to the data breach. Unable to prove that the CafePress data breach caused him an actual injury, Fus lacks standing to pursue this action and CafePress's motion to dismiss for lack of subject-matter jurisdiction is granted.

CONCLUSION

For the foregoing reasons, CafePress's motion to dismiss (Dkt. No. 17) is granted and Fus's motion to strike the declarations submitted by CafePress in support of its motion to dismiss

(Dkt. No. 31) is denied. This case is dismissed without prejudice for lack of subject-matter jurisdiction. Consequently, CafePress's motion to compel arbitration (Dkt. No. 45) is denied as moot.

ENTERED:

A handwritten signature in black ink, appearing to read "Andrea R. Wood", written over a horizontal line.

Andrea R. Wood
United States District Judge

Dated: November 30, 2020