UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

FARDOES KHAN,

Plaintiff,

v.

CHILDREN'S NATIONAL HEALTH SYSTEM,

Defendant.

Civil Action No. TDC-15-2125

MEMORANDUM OPINION

Plaintiff Fardoes Kahn has filed a putative class action against Children's National Health System ("CNHS"), asserting various statutory and common law causes of action related to a data breach at a CNHS hospital. Pending is the Motion to Dismiss filed by CNHS. The Motion is fully briefed and ripe for disposition. No hearing is necessary to resolve the issues. *See* D. Md. Local R. 105.6. For the reasons set forth below, the Motion is GRANTED IN PART and DENIED IN PART.

BACKGROUND

I. Data Breach

Khan receives treatment at Children's Hospital in Washington, D.C., a hospital operated by CNHS. Khan provided CNHS with personally identifiable information such as her date of birth, Social Security number, address, and telephone number. CNHS also maintains records containing Khan's private health care information such as diagnoses, treatment records, and health insurance information.

On or about July 26, 2014, hackers gained access to the email accounts of certain CNHS employees when those employees responded to "phishing" emails. The hackers' infiltration was not detected until December 26, 2014. During the five intervening months, the "email accounts had been potentially exposed in a way that may have allowed hackers to access information contained in those email accounts." Compl. ¶ 13. The email accounts contained certain patient information, such as names, addresses, dates of birth, Social Security numbers, and telephone numbers, as well as private health care information. On February 26, 2015, CNHS sent a letter to approximately 18,000 patients, including Khan, notifying them that their personal data may have been contained in these email accounts.[1] CNHS stated that the data breach did not extend to its electronic medical records system or patient charts and professed to have "no evidence that the information in the emails has been misused or even accessed." Def.'s Mot. Dismiss Ex. A, Data Breach Letter.

Khan alleges that her sensitive personal information was "compromised, viewed, and/or stolen" because CNHS did not take sufficient steps to protect it through encryption, passwords, or other measures. Compl. ¶¶ 20-21; 109. Upon learning of the breach, she placed passwords on her bank and credit card accounts. She remains concerned that her personal information will be misused, but she does not claim that she or anyone else affected by the data breach has learned of any misuse to date.

II. Procedural History

Khan filed suit in the Circuit Court for Montgomery County, Maryland on June 1, 2015, alleging violations of the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-

[1] CNHS attached the notification letter to its Motion, and the Court considers the letter because it is integral to the Complaint and of undisputed authenticity. *See Philips v. Pitt Cty. Mem'l Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009).

301 to 13-501 (2013), and the District of Columbia Consumer Protection Procedures Act, D.C. Code Ann., §§ 28-3901 to 28-3913 (2013), as well as negligence, breach of implied contract, and unjust enrichment. On July 21, 2015, CNHS removed the case to this Court under the Class Action Fairness Act, 28 U.S.C. § 1332(d) (2012). On September 8, 2015, CNHS filed a Motion to Dismiss. On October 16, 2015, Khan submitted an Opposition to the Motion. On November 16, 2015, CNHS filed a Reply. On December 29, 2015, Khan submitted a Motion for Leave to File a Surreply. Because the proposed surreply brief does not address "matters presented to the court for the first time in the opposing party's reply," *Khoury v. Meserve*, 268 F. Supp. 2d 600, 605 (D. Md. 2003), and because the issue discussed in the proposed surreply brief need not be addressed to resolve the Motion to Dismiss, the Motion for Leave to File a Surreply is denied. Khan and CNHS both submitted Notices of Supplemental Authority alerting the Court to recent decisions involving standing to sue for data breaches. The Court has reviewed and considered those cases.

DISCUSSION

CNHS argues that the Complaint should be dismissed for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) because Khan lacks standing, or, in the alternative, for failure to state a claim under Rule 12(b)(6). Because the Court finds, for the reasons stated below, that Khan lacks standing and that the Court thus lacks subject matter jurisdiction, it does not address the merits of Khan's claims. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94-95 (1998).

I. Legal Standards

A. Rule 12(b)(1)

It is the plaintiff's burden to show that subject matter jurisdiction exists. *Evans v. B.F. Perkins Co., Div. of Standex Int'l Corp.*, 166 F.3d 642, 647 (4th Cir. 1999). Federal Rule of Civil Procedure 12(b)(1) allows a defendant to move for dismissal based upon the belief that the plaintiff has failed to make that showing. When, as in this case, a defendant asserts that the plaintiff has failed to allege facts sufficient to establish subject matter jurisdiction, the allegations in the complaint are assumed to be true under the same standard as in a Rule 12(b)(6) motion, and "the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009).

B. Article III Standing

Article III of the Constitution limits the judicial power of the federal courts to actual "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 1. To invoke this power, a litigant must have standing. *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2661 (2013). The plaintiff bears the burden of proving standing. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). A plaintiff must establish (1) an injury in fact (2) fairly traceable to the challenged conduct (3) that is likely to be "redressed by a favorable judicial decision." *Hollingsworth*, 133 S. Ct. at 2661. In a class action, the court analyzes the injuries alleged by the named plaintiffs, not unnamed members of the potential class, to determine whether the plaintiffs have Article III standing. *Warth v. Seldin*, 422 U.S. 490, 502 (1975); *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

CNHS limits its attack on Khan's standing to the first element: injury in fact. An injury in fact requires "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at

561 (internal quotation marks and citations omitted). The United States Supreme Court articulated the standard for a future injury qualifying as an injury in fact in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), a case in which the Court held that attorneys and human rights, labor, legal, and media organizations lacked standing to challenge a foreign intelligence surveillance program based on possible future interception of their phone calls, because the plaintiffs' alleged injury depended upon an "attenuated chain of possibilities": the government would have to select the plaintiffs' clients and sources for surveillance, the Foreign Intelligence Surveillance Court would have to approve the proposed surveillance, and the plaintiffs' communications would actually have to be intercepted. *Id.* at 1148. The Court held that a threatened future injury "must be *certainly impending* to constitute an injury in fact" and that allegations of "*possible* future injury are not sufficient." *Id.* at 1147 (emphasis in original). The Court noted, however, that plaintiffs need not demonstrate that it is "literally certain" that they will suffer harm, and it acknowledged that "we have found standing based on a 'substantial risk' that the harm will occur." *Id.* at 1150 n.5 (quoting *Monsanto Co. v. Geertson Seed Farms,* 130 S. Ct. 2743, 2754-55 (2010)). Thus, "[a]n allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper*, 133 S. Ct. at 1147, 1150 n.5)).

II. Injury in Fact

Khan alleges several injuries that she contends establish Article III standing. She alleges that (1) she faces an imminent threat of identity theft; (2) she expended time and incurred out-of-pocket expenses to monitor her credit and otherwise protect against identity theft; (3) she has suffered a loss of privacy; (4) she has been deprived of the value of her personally identifiable

information; (5) the data breach has diminished the value of the services she receives from CNHS; (6) CNHS provided an inaccurate and delayed notification of the data breach; and (7) CNHS has violated various statutes and the common law.

A. Increased Risk of Identity Theft

Khan's most promising argument that she has an injury in fact to support Article III standing is that the data breach has placed her at an increased risk of identity theft. Neither the United States Court of Appeals for the Fourth Circuit nor any district court within the Fourth Circuit has addressed the standing of data breach victims. The issue, however, has been frequently litigated in federal courts in recent years, with different results. Two circuits, the United States Courts of Appeals for the Seventh and Ninth Circuits, have found standing for victims of data breaches based on the increased risk of identity theft. In *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), a case predating *Clapper*, a thief stole a laptop computer containing the unencrypted names, addresses, and Social Security numbers of 97,000 Starbucks employees, which led Starbucks to notify those employees of the theft and offer credit monitoring services, even though there had been "no indication that the private information has been misused." *Id.* at 1140-41. One named plaintiff, however, alleged that in the month following the theft someone used his Social Security number to attempt to open a bank account. *Id.* at 1141. The court, noting that "the possibility of future injury may be sufficient to confer standing on plaintiffs," held that the increased risk of identity theft was an injury in fact because the plaintiffs had alleged "a credible threat of real and immediate harm stemming from the theft of the laptop." *Id.* at 1142-43.

Following *Clapper*, the Seventh Circuit found standing stemming from hackers' use of malware to collect credit card data from up to 350,000 credit card customers of Neiman Marcus,

a luxury department store. *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 690 (7th Cir. 2015). In *Remijas*, Neiman Marcus learned that some of its customers had already found fraudulent charges on their credit cards before alerting the public about the data breach. *Id.* at 689-90. Approximately 9,200 of those cards were known to have been used fraudulently in the wake of the breach. *Id.* at 690. The court found that plaintiffs who alleged fraudulent charges on their credit cards had standing based on the time and expense necessary to resolve those charges. *Id.* at 692. Acknowledging that *Clapper* requires a "certainly impending" future injury, or at least a "substantial risk" of injury, the court found that plaintiffs who had not experienced fraudulent charges also had standing because those plaintiffs knew, from the numerous cards already used fraudulently, that their personal information had been stolen by individuals who intended to misuse it. *Id.* at 693-94 (questioning why the hackers would "break into a store's database" other than "to make fraudulent charges or assume those consumers' identities"); *see also Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-3700, 2016 WL 1459226, at *3-4 (7th Cir. Apr. 14, 2016) (following *Remijas* and holding that where hackers stole customer credit card and debit card data from a restaurant chain, and a named plaintiff had already received a fraudulent charge, plaintiffs had standing to sue).

By contrast, the United States Court of Appeals for the Third Circuit, in *Reilly v. Ceridian*, 664 F.3d 38 (3d Cir 2011), held that plaintiffs alleging an injury in fact from an increased risk of identity theft lacked standing. *Id.* at 43. In *Reilly*, hackers "potentially gained access to personal and financial information" of 27,000 individuals stored on the computer system of a payroll processing company. *Id.* at 40. It was unclear "whether the hacker read, copied, or understood" the plaintiffs' data. *Id.* After determining what information the hacker "may have accessed," the company sent letters to the potential identity theft victims informing

them of the breach and offering to provide one year of free credit monitoring and identity theft protection. *Id.*

Although *Reilly* predated *Clapper*, the Third Circuit applied the same standard later endorsed in *Clapper*, that the "threatened injury must be 'certainly impending'" in order to support standing. *Id.* at 42 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The court found that the increased risk of identity theft was "too speculative" to establish standing. *Id.* at 43. Distinguishing *Krottner*, in which someone had already attempted to open a bank account using stolen personal information, the court noted that there was no indication that the personal data had been or ever would be misused. *Id.* at 43-44. Rather, the threat of future injury was premised on the "speculation" that the hackers had (1) "read, copied, and understood" the personal information; (2) intended "to commit future criminal acts by misusing the information"; and (3) were able to use that information to the detriment of the plaintiffs. *Id.* at 42. The court thus found that this "string of hypothetical injuries" did not establish an "actual or imminent" injury necessary to confer standing. *Id.* at 44.

Although these courts reached conflicting results, the difference appears to arise not from the application of a different legal standard, but rather from crucial distinctions in the underlying facts. In *Krottner* and *Remijas*, the allegations included either actual examples of the use of the fruits of the data breach for identity theft, even if involving victims other than the named plaintiffs, or a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud. In *Krottner*, one of the plaintiff's credit card numbers had been fraudulently used. 628 F.3d at 1142. In *Remijas*, the cyberattack involved malware that specifically sought to collect customer credit card data, and 9,200 credit card numbers had already been used fraudulently. 794 F.3d at 690-93. By contrast, in *Reilly*, neither of these

factors was present. "A firewall was penetrated," and hackers had "potentially gained access to personal and financial information," but it was not known if the hackers "read, copied, or understood the data." *Reilly*, 664 F.3d at 40, 44.

The majority of district courts faced with challenges to the standing of data breach victims follow this pattern. In the absence of specific incidents of the use of stolen data for identity fraud purposes, district courts have generally found that the increased risk of identity theft does not confer standing. *See, e.g., In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 955 (D. Nev. 2015) (listing cases). In fact, the only post-*Clapper* cases cited by Khan or uncovered by this Court in which data breach victims were found to have standing all included allegations indicating that some of the stolen data had already been misused, that there was a clear intent to use the plaintiffs' personal data for fraudulent purposes, or both.[2] *See Remijas*, 794 F.3d at 690; *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1157-59 (D. Minn. 2014) (holding that after the theft of credit card and personal data for 110 million customers, "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees" incurred by plaintiffs constituted injuries in fact); *In re Adobe Sys., Inc. Privacy Litig. (Adobe)*, 66 F. Supp. 3d 1197, 1206, 1214-16 (N.D. Cal. 2014) (finding that the plaintiffs had standing where hackers used Adobe's system to decrypt the plaintiffs' credit card information and posted some of the stolen data, including Adobe source code, on the

[2] Some pre-*Clapper* decisions held that data breach victims had standing even without allegations of misuse or other indications of an intent to use the data for fraudulent purposes. *Ruiz v. Gap, Inc.*, 380 F. App'x 689, 691 (9th Cir. 2010); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 631, 634 (7th Cir. 2007); *McLoughlin v. People's United Bank, Inc.*, No. CIVA 308CV-00944 VLB, 2009 WL 2843269, at *1, 4 (D. Conn. Aug. 31, 2009); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 276, 280 (S.D.N.Y. 2008); *In re Dep't of Veterans Affairs Data Theft Litig.*, No. MDL 1796, 2007 WL 7621261, at *1, 3 (D.D.C. Nov. 16, 2007). None of these cases applied the "certainly impending" or "substantial risk" standards articulated by *Clapper*.

internet); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 955-58, 962-63 (S.D. Cal. 2014) (finding that the plaintiffs had standing where, following the hacking and theft of personal information of Sony customers, one of the named plaintiffs alleged fraudulent charges to his credit card); *see also Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *1, 3 (C.D. Cal. June 15, 2015) (finding that the plaintiffs had standing where hackers posted their personal information on file-sharing websites for identity thieves and used it to send the plaintiffs threatening emails); *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *2, 5-6 (N.D. Ill. July 14, 2014) (finding standing where the plaintiffs alleged that a named plaintiff in a different class action victimized by the same data breach suffered fraudulent charges on her credit card).

By contrast, several district courts have joined *Reilly* in dismissing suits where the plaintiffs, even where they alleged that their personal data had been stolen or accessed,[3] did not allege actual misuse of the data. *See In re Zappos.com, Inc.*, 108 F. Supp. 3d at 958-59 (finding no standing where the last four digits of credit card numbers of 24 million customers were stolen, but there were no allegations of unauthorized purchases or other signs of misuse); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 363, 366 (M.D. Pa. 2015) (finding no standing even though there was confirmation that hackers had breached a payroll company's computer system and that confidential, personal information was "accessed," where there was "no allegation that the hacker caused a new bank account or credit card to be opened in any of Plaintiffs' names, or any other form of identity theft"); *In re Science Applications Int'l Corp. Backup Tape Data Theft Litig. (SAIC)*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014) (finding standing only as to individual

[3] When Khan's Complaint is viewed in its entirety, including Khan's allegation that the data was "compromised, viewed, *and/or* stolen," Compl. ¶ 109 (emphasis added), it is evident that it is not known whether the plaintiffs' personal data was actually removed by the hackers.

plaintiffs who had alleged actual misuse of their personal data); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 656 (S.D. Ohio 2014) (finding no standing even though personal information was stolen from an insurance company's computer network and was actually disseminated); *see also In re SuperValu, Inc.*, 2016 WL 81792, at *5 (finding that an allegation of a single fraudulent charge in the year and a half following a data breach was not traceable to the data breach and did not support an inference that plaintiffs' credit card information was at substantial risk of misuse because of the breach); *Green v. eBay Inc.*, No. CIV.A. 14-1688, 2015 WL 2066531, at *4-6 (E.D. La. May 4, 2015) (finding no standing where hackers accessed eBay's files containing users' personal information).

The Court therefore concludes that in the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud. Under this framework, Khan's allegations fall short. Unlike in *Krottner* or *Remijas*, Khan alleges no facts indicating that the hackers have attempted to engage in any misuse of CNHS patients' personal information since the breach was discovered. She alleges no suspicious activity: no unauthorized bank accounts or credit cards, no medical fraud or identity theft, and no targeted solicitations for health care products or services.

Nor do the circumstances of the data breach clearly indicate that the hackers' purpose was to use patients' personal data to engage in identity fraud. Unlike in *Remijas*, where malware was deployed on Neiman Marcus's computer system in an attempt to collect credit card data, 794 F.2d at 690, or *Adobe*, where the hackers specifically removed and decrypted customers'

personal data, 66 F. Supp. 3d at 1206, here the data breach consisted of the use of phishing emails to gain access to the email accounts of certain CNHS employees, not its electronic medical records system or some other centralized database of personal data. Although these email accounts contained some patients' personal information, there is no indication that the patients' personal data was actually viewed, accessed, or copied, or was even the target of the phishing scheme. Tellingly, Khan, although at times referring to the data as "stolen," alleges only that hackers had "unauthorized access" to the email accounts, that the accounts were "*potentially* exposed in a way that *may* have allowed hackers to access information contained in those email accounts," and that the data was "readily able to be copied." Compl ¶¶ 13-22 (emphasis added). Thus, the allegations are more akin to those in *Reilly*, where the hackers "potentially gained access to personal and financial information," but it was unclear "whether the hacker read, copied, or understood" the plaintiffs' personal data, and there was no indication of actual misuse. *Reilly*, 664 F.3d at 38-40; *cf. SAIC*, 45 F. Supp. 3d at 25 (finding no standing absent specific allegations of data misuse where data was on stolen backup tapes and there was no information on whether the thief was actually seeking to extract personal data to commit identity fraud). In both cases, it is not clear whether the data breach targeted the plaintiffs' data, as opposed to other sensitive information contained in the email accounts or the electronic files.

Khan's more general allegations—that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft—do not alter this conclusion. These specific statistics, which are cited in numerous other cases, do not by themselves establish that there is "certainly impending" harm under the specific facts of a given case. *See, e.g.*, *SAIC*, 45 F. Supp. 3d at 25-26; *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 877 (N.D. Ill. 2014); *Green*, 2015 WL 2066531, at *5. Because the

Complaint does not allege either actual misuse of the personal data or facts indicating a clear intent to engage in such misuse with plaintiffs' data, the Court finds that Khan has not alleged a "certainly impending" injury or "substantial risk" of imminent injury sufficient to establish Article III standing. *See Clapper*, 133 S. Ct. at 1147, 1150 n.5.

B. Additional Grounds for Standing

Khan's additional claims of injury in fact are unpersuasive. First, she asserts that the expense of guarding against identity theft constitutes injury in fact. However, incurring costs as a reaction to a risk of harm does not establish standing if the harm sought to be avoided is not itself "certainly impending." *Clapper*, 133 S. Ct. at 1151; *Reilly*, 664 F.3d at 46; *In re SuperValu, Inc.*, 2016 WL 81792, at *7 (stating that "the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent").

Second, Khan argues that the data breach has caused a loss of privacy that constitutes an injury in fact. However, she has not identified any potential damages arising from such a loss and thus fails to allege a "concrete and particularized injury." *See In re Zappos.com, Inc.*, 108 F. Supp. 3d at 962 n.5.

Third, Khan claims injury based on the theory that she contracted with CNHS to secure her personal information, and that its failure to do so deprived her of the full value of the services for which she paid. Khan, however, acknowledges that she purchased "surgery and treatment" from CNHS. Compl. ¶ 9. She does not allege any facts showing that she overpaid for those services or that she would have sought those services from another provider had she been aware of the hospital's allegedly lax data security. *See SAIC*, 45 F. Supp. 3d at 30 (rejecting a similar

theory because the plaintiffs "have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid").

Fourth, Khan alleges that the value of her personally identifiable information has been diminished by the data breach. She does not, however, explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information. *See id.* at 30 (rejecting this theory in part because plaintiffs did not claim that they intended to sell their own personal information on the cyber black market). Her analogy to the theft of a family heirloom is unconvincing since the data breach has not deprived her of the use of her personal information.

Fifth, Khan claims that CNHS's notification letter "was misleading in that it provided vague descriptions of what was stolen and falsely implied that there was no risk from the data breach." Compl. ¶ 66. The letter, however, expressly encouraged victims to take steps to mitigate risks from the breach. Even if Khan was misled, she points to no concrete injury caused by the letter. She acknowledges that she took preventive action after receiving the letter and has not suffered from any actual misuse of her personal data. Similarly, Khan's claim that CNHS impermissibly delayed notifying her of the breach does not establish any injury, since Khan does not claim that the period during which she was unaware of the need to monitor for identity fraud resulted in any harm. *See SAIC*, 45 F. Supp. 3d at 30-31.

Finally, Khan contends that the violations of state statutes and common law alleged in the Complaint establish standing. Khan conflates the question whether she has a cause of action under state law with the question whether she has Article III standing to pursue that cause of action in federal court. *See Steel Co.*, 523 U.S. at 96–97 (distinguishing statutory standing from Article III standing); *CGM, LLC v. BellSouth Telecomms., Inc.*, 664 F.3d 46, 51-52 (4th Cir.

2011) (same). "Article III standing requires a concrete injury even in the context of a statutory violation." *Spokeo, Inc. v. Robins*, No. 13-1339, 578 U.S. __ , slip op. at 9 (2016). Although "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law,'" *id.* (quoting *Lujan*, 504 U.S. at 578), a "bare procedural harm" under a federal statute, "divorced from any concrete harm," would not "satisfy the injury-in-fact requirement," *id.* at 9-10. Here, where Khan alleges violations of state law, she advances no authority for the proposition that a state legislature or court, through a state statute or cause of action, can manufacture Article III standing for a litigant who has not suffered a concrete injury. *See Hollingsworth v. Perry,* 133 S. Ct. at 2667-68 (2013) (holding that a state supreme court decision finding that official proponents of a ballot initiative have authority to defend the legality of that initiative did not vest those proponents with Article III standing because states cannot alter the role of the federal judiciary established by Article III "simply by issuing to private parties who otherwise lack standing a ticket to the federal courthouse"); *Lee v. American Nat'l Ins. Co.*, 260 F.3d 997, 1001-02 (9th Cir. 2001) ("[A] plaintiff whose cause of action is perfectly viable in state court under state law may nonetheless be foreclosed from litigating the same cause of action in federal court, if he cannot demonstrate the requisite injury."). Moreover, Khan has failed to connect the alleged statutory and common law violations to a concrete harm.

Because Khan has not alleged an injury in fact as required to establish Article III standing, the Court concludes that it lacks subject matter jurisdiction. In the absence of jurisdiction, the Court does not consider the remaining arguments in the Motion.

III. Remand

"If at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." 28 U.S.C. § 1447(c) (2012). "The plain language of

§ 1447(c) gives 'no discretion to dismiss rather than remand an action' removed from state court over which the court lacks subject-matter jurisdiction." *Roach v. W. Va. Reg'l Jail & Corr. Facility Auth.*, 74 F.3d 46, 49 (4th Cir. 1996) (*quoting Int'l Primate Prot. League v. Adm'rs of Tulane Educ. Fund*, 500 U.S. 72, 89 (1991)). The Court declines CNHS's invitation to ignore the plain language of the statute and dismiss the case. This case will be remanded to state court.

CONCLUSION

For the foregoing reasons, CNHS's Motion to Dismiss is GRANTED IN PART and DENIED IN PART. The Court finds that Khan lacks standing, but it does not dismiss her claims. Instead, the case is REMANDED to state court. A separate Order shall issue.

Date: May 18, 2016

THEODORE D. CHUANG
United States District Judge