UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

ALEXANDRIA RUDOLPH, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

HUDSON'S BAY COMPANY, SAKS FIFTH AVENUE LLC, SAKS & COMPANY LLC, SAKS INCORPORATED and LORD & TAYLOR LLC,

Defendants.

----------x

18-cv-8472 (PKC)

OPINION AND ORDER

CASTEL, U.S.D.J.

In November 2017, plaintiff Alexandria Rudolph used her Visa-issued debit card to make purchases at a Saks OFF 5TH store in Beverly Hills, California. The card was linked to an account that Rudolph maintained at Bank of America. In May 2018, Bank of America notified Rudolph of suspected fraudulent activity on her card and temporarily froze the account. Rudolph incurred no fraudulent charges, her account was soon unfrozen and she quickly obtained a replacement card at a branch location of the bank.

The previous month, in April 2018, it was publicly disclosed that a group of hackers had breached the payment-card databases of defendants Saks Fifth Avenue LLC, Saks & Company LLC, Saks Incorporated and Lord & Taylor LLC, all of which are owned by a parent company, defendant Hudson's Bay Company ("Hudson's"). The breach was limited to the names and account numbers of customer credit and debit cards. There is no allegation that hackers accessed other types of information, like social security numbers, site passwords, birth dates or contact information.

Rudolph now brings this putative class action asserting state law claims directed to the breach of her debit-card data. According to the Complaint, Rudolph is at a substantially increased risk of future fraud or identity theft due to hackers' possession of her card data, and she has a continuing interest in protecting that data from misuse. Rudolph also asserts that she was injured due to the expenditure of time in dealing with the breach and obtaining a new debit card, as well as the out-of-pocket expense of the gasoline that was needed to drive 25 miles to a Bank of America branch when she obtained the new card.

Defendants move to dismiss the Second Amended Complaint (the "Complaint") for failure to allege subject matter jurisdiction and failure to state a claim, pursuant to Rules 12(b)(1) and 12(b)(6), Fed. R. Civ. P. They urge that Rudolph has not adequately alleged an existing injury-in-fact or an actionable risk of future injury, as required to demonstrate Article III standing. They argue that Rudolph has described a data breach limited to the name and account number of a since-canceled debit card, which does not plausibly put her at risk of future injury. Defendants further contend that Rudolph has not adequately alleged why the mitigation and monitoring efforts that she undertook upon learning of the breach were reasonable and necessary; they note that her bank immediately canceled the debit card and no fraudulent were charges incurred.

Courts, including the Second Circuit, have looked to the facts surrounding a data breach when deciding whether a complaint adequately alleges a risk of future injury and the plaintiff's claim for compensable mitigation expenses. See, e.g., Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 90 (2d Cir. 2017) (summary order). For the reasons that will be explained, the Court concludes that the Complaint has failed to allege that Rudolph is at a substantial risk of future injury. However, the time and expense that she expended in order to

obtain a replacement debit card are sufficient to satisfy the "low threshold" required to allege injury-in-fact and demonstrate Article III standing. See John v. Whole Foods Mkt. Grp., Inc., 858 F.3d 732, 736 (2d Cir. 2017).

Defendants' motion to dismiss pursuant to Rule 12(b)(6) is granted as to Rudolph's claim for negligence per se, her claim under the Declaratory Judgment Act, her claim under Mississippi's consumer-protection statute, and her notice-based claim under California's Customer Records Act, but is otherwise denied.

DISCUSSION.

A. The Breach of Customer Data at Hudson's Stores.

On March 28, 2018, a hacking group variously known as "JokerStash" or "Fin7" announced that it had successfully gained unauthorized access to the data of more than five million credit and debit cards in the possession of an unnamed corporation. (Compl't ¶ 2.) On April 1, 2018, a cyber-threat research group called Gemini Advisory ("Gemini") reported that the data was stolen from defendant Hudson's, the parent company of the defendant retailers in this case. (Compl't ¶ 3.)

Gemini stated that the hack took place in the retailers' point-of-sale ("POS") systems. (Compl't ¶ 4.) POS systems store data from the magnetic strip of a credit or debit card, including the cardholder's name, the card's expiration date and its security code. (Compl't ¶ 4.) The Complaint alleges that the breach went undetected for nearly a year, and that defendants learned of the breach only after it was announced by Gemini. (Compl't ¶ 83.)

Following Gemini's report, Hudson's confirmed that hackers had gain unauthorized access to data held by that certain of its Saks and Lord & Taylor stores in North America. (Compl't ¶ 6.) According to the Complaint, the defendants' inadequate security

measures contributed to the breach, as it was widely known across the retail industry and within Hudson's itself that POS systems were vulnerable to malicious hacking. (Compl't ¶¶ 13-16, 56-66, 98.) For example, in the months before the JokerStash/Fin7 breach, a news report stated that personal data for tens of thousands of Saks Fifth Avenue customers was available online. (Compl't ¶ 76.) The Complaint also alleges that defendants failed to comply with FTC guidance and industry best practices on data security. (Compl't ¶¶ 67-74, 99-100.)

B. The Effect of the Data Breach on Plaintiff Rudolph.

On November 23, 2017, Rudolph used a Visa-issued debit card to purchase items at a Saks OFF 5th retail store in Beverly Hills, California. (Compl't ¶ 21.) On May 18, 2018, Bank of America notified Rudolph of suspected fraudulent activity on the same debit card, and froze Rudolph's account. (Compl't ¶ 22.)

According to the Complaint, Rudolph spent approximately 20 minutes on the phone with Bank of America before driving 25 miles to visit a branch in person so that she could obtain a new debit card. (Compl't ¶ 22.) The Complaint describes approximately four hours of activity undertaken by Rudolph to obtain a new debit card, review her account records and update her payment information with retailers, plus an additional "several hours" of reviewing financial statements for suspicious charges. (Compl't ¶ 22.) The Complaint also alleges that Rudolph incurred approximately $4.68 in gasoline costs to drive to the bank. (Compl't ¶ 22.)

The Complaint lists injuries that Rudolph claims as a result of the data breach. (Compl't ¶¶ 25-27, 101.) They include imminent and impending injury arising from the increased risk of future fraud and identity theft stemming from the data breach; the time and money lost in obtaining a new debit card and dealing with the data breach; the purchase of items that she would not have bought had she known defendants lacked adequate data-security

practices; and the "diminution in the value of her Customer Data." (Compl't ¶¶ 25-27, 101.) The Complaint states that defendants' failure to secure customer data has had "severe" ramifications, and that identity theft broadly can lead to a variety of frauds, including wrongful bank-account access, immigration fraud or obtaining a fake driver's license. (Compl't ¶¶ 88-92.)

C. Procedural History.

This action was originally filed in the Central District of California and was transferred to this District in September 2018. (Docket # 1, 46.) Subject matter jurisdiction is premised on the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). (Compl't ¶ 35.) According to the Complaint, the amount in controversy exceeds $5 million, exclusive of interest and costs; there are more than 100 putative class members; and at least one plaintiff and one defendant are citizens of different states. (Compl't ¶ 35.) The Complaint brings nine causes of action, including common law claims for breach of implied contract, negligence, negligence per se, unjust enrichment, and declaratory and injunctive relief. (Compl't ¶¶ 117-45, 156-190.) It brings claims under the California Customer Records Act, Cal. Civ. Code § 1798.81.5(a)(1), California's unfair competition law, Cal. Bus. & Prof. Code § 17200, and Mississippi's consumer protection statute, Miss. Code § 78-24-1. (Compl't ¶¶ 146-55, 191-214.)

Rudolph purports to bring claims on behalf of a putative class of all persons in the United States who made a purchase with a credit card or debit card at Saks Fifth Avenue, Saks OFF FIFTH or Lord & Taylor stores between March 2017 and March 2018. (Compl't ¶ 103.) She also seeks to bring claims on behalf of a subclass consisting of California residents who made the same transactions during the same time period. (Compl't ¶ 104.)

DISCUSSION.

I. Defendants' Rule 12(b)(1) Motion is Granted in Part and Denied in Part.

A. Rule 12(b)(1) Standard.

Rule 12(b)(1) permits a defendant to move to dismiss an action for lack of subject matter jurisdiction. A Rule 12(b)(1) motion may be either fact-based or facial. Carter v. HealthPort Techs., LLC, 822 F.3d 47, 56 (2d Cir. 2016). Here, defendants have moved to dismiss on the basis of the complaint, and no party relies on facts outside of the pleadings.

"When the Rule 12(b)(1) motion is facial, i.e., based solely on the allegations of the complaint or the complaint and exhibits attached to it . . . the plaintiff has no evidentiary burden." Id. The plaintiff "must allege facts that affirmatively and plausibly suggest that it has standing to sue." Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140, 145 (2d Cir. 2011). All reasonable inferences are to be drawn in favor of the plaintiff. Id. A district court must dismiss a complaint for lack of subject matter jurisdiction where a plaintiff does not have constitutional standing to bring the action. Cortlandt St. Recovery Corp. v. Hellas Telecommunications, S.A.R.L., 790 F.3d 411, 416-17 (2d Cir. 2015).

B. Whether a Plaintiff Has Alleged Injury as a Result of a Data Breach Turns on the Facts Unique to Each Case.

To successfully invoke federal subject matter jurisdiction, a plaintiff must demonstrate that she has Article III standing, which requires her to "clearly" allege that she "(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, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Id. at 1548 (quoting Lujan v. Defs. of

Wildlife, 504 U.S. 555, 560 (1992)). "For an injury to be particularized, it must affect the plaintiff in a personal and individual way," and in order to be "concrete," the injury "must actually exist." Id. (quotation marks omitted). The injury-in-fact requirement "helps to ensure that the plaintiff has a 'personal stake in the outcome of the controversy.'" Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)).

A plaintiff has Article III standing if she plausibly alleges future injury, provided that "the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." Susan B. Anthony List, 573 U.S. at 158; see also Hedges v. Obama, 724 F.3d 170, 188-89 (2d Cir. 2013) ("Actual injury-in-fact exists when a defendant's actions have inflicted a concrete, present harm on the plaintiff. But the Supreme Court has recognized that a plaintiff in some circumstances may have standing to sue even when the plaintiff shows only an imminent threat of future harm or a present harm incurred in consequence of such a threat.") (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)). An injury may include mitigation-related expenses "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Clapper, 568 U.S. at 414 n.5. A plaintiff does not demonstrate a substantial risk of harm by alleging an "attenuated chain of inferences" that might result in injury. Id.

"Whether the risk of identity theft is sufficiently material to create an injury in fact is 'a question for lower courts to determine in the first instance, on a case- and fact-specific basis.'" Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017) (Schofield, J.) (quoting Katz v. Donna Karan Co., L.L.C., 872 F.3d 114, 121 (2d Cir. 2017)). Sackin distinguished a breach of information "including birth dates and social security numbers" from a breach of "all or a portion of a credit card number," describing the former categories of

information as "far more sensitive" and heightening the risk of identity theft. Id. at 746-47; see also In re Zappos.com, Inc., 888 F.3d 1020, 1023, 1027-28 (9th Cir. 2018) (breach of "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information" included "information that could be used to help commit identity fraud or identity theft" and to "commander[]" online accounts, which was sufficient to allege threat of future injury).

The Second Circuit distinguished a breach of card-specific data from other forms of personal information in Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 90 (2d Cir. 2017) (summary order). In Whalen, defendant Michaels Stores publicly announced a possible breach of credit- and debit-card data. Id. at 90. The complaint alleged that approximately two weeks after plaintiff used her credit card at a Michaels store, a card with her account information was physically presented in Ecuador for two charges totaling more than $1,700. Id. The plaintiff brought claims against Michaels for breach of implied contract and violation of the New York General Business Law. Id.

Whalen affirmed the district court's conclusion that the plaintiff did not allege injury arising from a breach of card data, and therefore did not have Article III standing to pursue state law claims. Id. at 90-91. In an attempt to demonstrate injury, the Whalen plaintiff had alleged that her credit card information had been stolen and that two attempts to use it followed; that she risked future identity fraud; and that she had lost time and money when resolving the attempted fraudulent charges and monitoring her credit information. Id. The Second Circuit concluded that the Complaint failed to allege a concrete injury. Id. Plaintiff neither paid nor was asked to pay for the fraudulent charges; she did not identify a threat of future fraud, as her stolen

credit card had been canceled and no other identifying information was stolen; and the complaint did not allege the time and expense that she undertook to monitor her financial data. Id.

As a summary order, Whalen is not precedent that binds this Court, but it may be relied upon for its persuasive value. See, e.g., Brault v. Soc. Sec. Admin., Comm'r, 683 F.3d 443, 450 n.5 (2d Cir. 2012) ("We are, of course, permitted to consider summary orders for their persuasive value, and often draw guidance from them in later cases."); United States v. Payne, 591 F.3d 46, 58 (2d Cir. 2010) ("[d]enying summary orders precedential effect does not mean that the court considers itself free to rule differently in similar cases.") (quotation marks omitted).

C. Rudolph Has Not Plausibly Alleged a Substantial Risk of Future Harm.

As noted, a plaintiff may allege injury if she can demonstrate the "invasion of a legally protected interest" that is "imminent" and "concrete and particularized." Spokeo, 136 S. Ct. at 1547. This may include a showing of "substantial risk that the harm will occur," leading a plaintiff "to reasonably incur costs to mitigate or avoid that harm." Clapper, 568 U.S. at 414 n.5.

The data breach at issue in this case was limited to card-specific information. Hackers stole "'Track 1' and 'Track 2' data from the magnetic strip on the payment card, which includes the cardholder's first and last name, the expiration date of the card, and the CVV (three or four number security code on the card)." (Compl't ¶¶ 4, 50.) The Complaint alleges that the POS systems also retained card account numbers. (Compl't ¶ 41.) It alleges that once this information is obtained by a hacker, it can be used for online purchases or physically replicated in a card. (Compl't ¶ 54.) According to the Complaint, as a result of this breach, Rudolph and any putative class members "now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights." (Compl't ¶ 95.)

In contrast to some other data-breach cases, there is no allegation that the breach included information like home addresses, e-mail addresses, social security numbers or online passwords. When Bank of America learned of potentially fraudulent activity in Rudolph's debit card account, it froze the account, cancelled the card, and issued her a new one. The card number, the expiration date and the CVV security code of Rudolph's now-canceled card would appear to be worthless to anyone. Rudolph has not identified any plausible, remaining risk.

Whalen concluded that the plaintiff did "not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information – such as her birth date or Social Security number – is alleged to have been stolen." 689 Fed. App'x at 90. Other courts have distinguished the breach of payment-card data from breaches that disclose personal information that is more susceptible to acts of identity theft. In re SuperValu, Inc., 870 F.3d 763, 770-71 (8th Cir. 2017), concluded that plaintiffs did not allege a substantial risk of future identity theft when a data breach was limited to payment-card information, distinguishing such data from social security numbers, birth dates and drivers' license numbers. The "mere possibility" of future injury through misuse of payment-card data was not enough to demonstrate standing. Id. at 771.

Consistent with SuperValu and Whalen, other courts have concluded that a data breach that includes social security numbers, names, birth dates, e-mail addresses and other contact information, employment information, online passwords and account numbers can plausibly allege a substantial risk of future harm. See In re Zappos, 888 F.3d at 1027-28; Attias v. Carefirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 386 (6th Cir. 2016); In re Yahoo! Inc. Customer Data Sec. Breach Litig., 2017

WL 3727318, at *15 (N.D. Cal. Aug. 30, 2017) (distinguishing the payment-card breach in Whalen from a breach revealing broader categories of information).

Rudolph relies on Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966-67 (7th Cir. 2016), which concluded that two plaintiffs had alleged injury at the pleading stage based on a breach limited to payment-card information. Following a data breach at a national restaurant chain, four fraudulent charges were made on the debit-card account of one plaintiff, who immediately canceled his card and subscribed to a credit-monitoring service. Id. at 965. A second plaintiff did not have fraudulent charges; he did not cancel his card, and alleged that he spent time and effort monitoring card statements and credit reports. Id. The defendant argued that because the breach was limited to card data, it "posed a risk only of fraudulent charges to affected cards, not of identity theft." Id. at 967. Lewert characterized this as "a factual assumption that has yet to be tested," and explained that "[a]s a matter of pleading, nothing suggests that the plaintiffs' mitigation efforts were unreasonable." Id.; see also Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (complaint adequately alleged injury based on mitigation efforts following breach of card data held by Neiman Marcus chain).

Whalen distinguished Lewert and Remijas because the Whalen plaintiff did not allege "specifics" about the time and effort she spent monitoring her credit, and did not explain "how she can plausibly face a threat of future fraud" when the breached credit-card account had already been canceled. 689 Fed. App'x at 90-91 & n. 1. Here, the Complaint describes numerous injuries that could generally occur under a broad label of "identity theft" and a need for Hudson's and others to take proactive measures to protect customer data (Compl't ¶¶ 14-18, 43-74, 87-102), but it does not plausibly describe any threat to Rudolph that continued after her card was canceled. It does not describe how a data thief's possession of account numbers on a

canceled debit card would facilitate the types of identity theft recited in the Complaint as potential injuries, such as accessing medical treatment on Rudolph's insurance, committing immigration fraud, taking out a driver's license in Rudolph's name, filing fraudulent tax returns or wrongfully obtaining government benefits. (Compl't ¶¶ 90-91.) A complaint's use of the broad label "identity theft" does not substitute for a plausible allegation of substantial risk of injury in the future.

The Complaint also does not plausibly allege an imminent risk of any other harm arising from a misuse of Rudolph's canceled debit card. The card has been canceled, the account was immediately frozen, and no fraudulent charges were incurred. (Compl't ¶ 22.) Rudolph does not plausibly allege why the breach of data on her since-canceled card now requires "years of constant surveillance" to guard against a "continuing increased risk of harm from identity theft and identity fraud . . . ." (Compl't ¶¶ 95, 100.) The ongoing risks posed by access to more sensitive data like social security numbers, birth dates and account passwords are not described here.

A "subjective fear" or "speculative threat" is not enough to identify injury. Clapper, 568 U.S. at 416; see also Attias, 865 F.3d at 627-29 (plaintiff alleged injury based on mitigation expenses, including data-monitoring subscriptions, when data breach included social security numbers and put plaintiffs at substantial risk of future harm). The Court therefore concludes that the Complaint has not identified a "substantial risk" of future harm sufficient to demonstrate injury and Article III standing. Hedges, 724 F.3d at 188-89; Clapper, 568 U.S. at 414 n.5. To the extent that Rudolph's claims are premised on a substantial risk of future injury, the Court concludes that she has not demonstrated Article III standing.

D. Rudolph Has Alleged an Injury-in-Fact Based on the Time and Expense of Responding to the Breach and Obtaining a Replacement Card.

Rudolph also alleges that she was injured in fact at or around the time that she learned of the data breach and took measures to obtain a replacement debit card. She asserts that her injuries include time required to replace the card and the cost of gasoline needed to drive to a bank branch and retrieve the new card. (Compl't ¶ 22.) Rudolph does not allege that she was injured by any charge actually made to her debit account. See, e.g., In re SuperValu, 870 F.3d at 772-73 (plaintiff adequately alleged injury based on fraudulent account charge).

Identifying an injury-in-fact is "a low threshold." John v. Whole Foods Mkt. Grp., Inc., 858 F.3d 732, 736 (2d Cir. 2017) (Article III standing demonstrated where the plaintiff "adequately and plausibly allege[d] that Whole Foods overcharged him at least once for pre-packaged cheese and cupcakes."). In Diffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828-29 (7th Cir. 2018), the court concluded that a plaintiff demonstrated injury based on allegations that a data breach required her to "spend time sorting things out with the police and her bank," noting that "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective." Diffenbach also observed that "[m]any people use credit or debit cards to pay bills automatically; every time the account number changes, these people must devote some of their time and mental energy to notifying merchants that the old numbers are invalid and new ones must be used." Id. at 827.

District courts have also recognized Article III standing based on incidental costs that arise when a card must be replaced or an account has been frozen to protect against a breach. Torres v. Wendy's International, LLC, 2017 WL 8780453, at *2 (M.D. Fla. Mar. 21, 2017), concluded that the plaintiff demonstrated "economic harm . . . sufficient to allege standing" based on a $3 late fee on a utility bill, which apparently arose from an account freeze following a

breach. And in Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1241 (D. Colo. 2018), the district court adopted a magistrate judge's recommendation that a plaintiff demonstrated injury-in-fact by way of time spent obtaining a new debit card, the $45 cost to expedite its delivery, and loss of cash-back rewards plaintiff might otherwise have accrued.

According to Rudolph, when she learned that a hold had been placed on her debit card, she spent about twenty minutes on the phone with a Bank of America representative. (Compl't ¶ 22.) She then drove to a Bank of America branch and physically retrieved a new card, which took about 90 minutes of travel time. (Id.) The drive used approximately 1.2 gallons of gas, which cost her around $4.68. (Id.) Rudolph states that she drove to the bank branch because she "needed a new debit card immediately . . . ." (Id.)

At the bank, Rudolph spent approximately 30 minutes speaking to an employee about the account freeze and her need for a new card. (Id.) Rudolph later spent an additional hour reviewing her records and another 30 minutes updating her payment card information with retailers. (Id.) In all, Rudolph alleges that she expended approximately 230 minutes and $4.68 to deal with the freeze placed on her card and obtain a replacement debit card. (Id.)

Defendants urge that the time and expense of obtaining a replacement card do not amount to an injury in fact. They point out that no fraudulent charge was incurred, and that Bank of America acted before Rudolph was even aware that her account was at risk. (Def. Mem. at 7-8.) The Complaint alleges that Rudolph drove to a Bank of America branch to retrieve a new card in person because she needed one "immediately," (Compl't ¶ 22) but defendants urge that this does not demonstrate injury because Rudolph does not explain why she needed a new debit card immediately, as opposed to waiting for a card to arrive in the mail. (Def. Mem. at 8-9.)

Defendants also rely on Whalen, which concluded that the plaintiff did not allege sufficient facts to demonstrate injury based on the time and expense spent to monitor her credit. Whalen noted that the plaintiff pleaded "no specifics" about the time and effort she expended, and the Complaint alleged only that "'the Class suffered additional damages based on the opportunity cost and value of time that [she] and the Class have been forced to expend to monitor their financial and bank accounts.'" 689 Fed. App'x at 91.

In describing injuries related to obtaining a replacement debit card, Rudolph has identified a concrete and particularized loss based on actual time spent responding to the breach and obtaining a new debit card. Rudolph's complaint offers a level of detail that was absent from Whalen, and also describes a category of injury that is different than mitigation and monitoring time, one based on the identifiable, already-incurred loss of time and money. The Court concludes that the Complaint's description of the time and expense lost by Rudolph in or about May 2018 is sufficient to demonstrate injury and Article III standing.

The defendants' Rule 12(b)(1) motion is therefore denied as to the time and expense directly attributable to the replacement of Rudolph's debit card.

E. Rudolph Has Not Alleged Injury-in-Fact Based on Diminution of Her Customer Data.

Rudolph separately asserts that she suffered actual injury based on "damages to and diminution in the value of [her] Customer Data," which the Complaint describes as intangible property that she entrusted to defendants. (Compl't ¶¶ 17(h), 26.) The Complaint defines "Customer Data" as debit and credit card numbers collected at the time consumers made purchases at the defendant retailers. (Compl't ¶ 1.)

Courts have reached differing conclusions on whether personal information like names, e-mail addresses, telephone numbers, birth dates, passwords and security questions have

a sales value that can be diminished if it is obtained by hackers. See, e.g., Yahoo!, 2017 WL 3727318, at *13-14 (plaintiffs plausibly alleged injury based on diminution in the market value of personal data); Remijas, 794 F.3d at 695 (declining to recognize "standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.").

Here, the Complaint does not allege the existence of a market for Rudolph's debit card information or how the value of such data could have decreased because of a breach. Any allegation that Rudolph was injured through the diminution in value of account numbers on her canceled debit card is conclusory, and does not demonstrate injury-in-fact.

The Court therefore concludes that the claimed diminution in the value of her personal information does not support Article III standing.

F. Rudolph Has Not Alleged Injury-in-Fact Based on the Temporarily Inability to Access Her Funds.

Rudolph also asserts that she was injured based on the "loss of use of and access" to her account funds during the time that a freeze was in effect. (Compl't ¶ 17(e).) She makes this allegation on behalf of herself and members of the putative class, and states that injury arose from "adverse effects on their credit," missed payments and late fees. (Id.; emphasis added.)

However, Rudolph does not identify any such injury that arose from the brief freeze placed on her own account. Absent an allegation of how an account freeze resulted in a loss to Rudolph, the claim that she was injured by the temporary inability to access her account does not demonstrate injury.

G. Rudolph Has Not Alleged a "Benefit-of-the-Bargain" Injury.

Lastly, Rudolph alleges that she never would have made a purchase at Saks OFF 5TH if she had known that defendants lacked adequate data security. (Compl't ¶ 23.) She

alleges that she suffered injury when she paid for products that she would not have purchased had defendants disclosed their insufficient security practices. (Compl't ¶ 25.)

"In data storage and collection cases, courts have consistently rejected as too tenuous to support an injury-in-fact claims that a defendant's failure to comply with the law, or to prevent an actual data breach, diminished the 'benefit-of-the-bargain.'" Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 518 (S.D.N.Y.) (Koeltl, J.) (collecting cases), vacated in part on other grounds, 717 Fed. App'x 12 (2d Cir. 2017). The items that Rudolph purchased from Saks OFF 5TH are not identified in the Complaint, but there is no allegation that they were deficient or did not meet expectations as a result of the data breach. See id.

The Court therefore concludes that the claimed benefit-of-the-bargain injury does not support Article III standing.

II. Defendants' Rule 12(b)(6) Motion Is Granted in Part and Denied in Part.

A. Rule 12(b)(6) Standard.

Rule 12(b)(6) requires a complaint to "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007)). In assessing the sufficiency of a pleading, a court must disregard legal conclusions, which are not entitled to the presumption of truth. Id. Instead, the Court must examine the well-pleaded factual allegations and "determine whether they plausibly give rise to an entitlement to relief." Id. at 679. "Dismissal is appropriate when 'it is clear from the face of the complaint, and matters of which the court may take judicial notice, that the plaintiff's claims are barred as a matter of law.'" Parkcentral Global Hub Ltd. v. Porsche Auto. Holdings SE, 763 F.3d 198, 208-09 (2d Cir. 2014) (quoting Conopco, Inc. v. Roll Int'l, 231 F.3d 82, 86 (2d Cir. 2000)).

B. California Choice-of-Law Standards Govern Rudolph's Claims.

This action was originally filed in the Central District of California and transferred to this District pursuant to 28 U.S.C. § 1404. (Docket # 45.) While a federal court sitting in diversity ordinarily applies the choice-of-law rules of the state where it sits, if an action has been transferred pursuant to section 1404, "the state law applicable in the original court also appl[ies] in the transferee court." Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Texas, 571 U.S. 49, 65 (2013). This exception is necessary to prevent 'defendants, properly subjected to suit in the transferor State,' from 'invok[ing] § 1404(a) to gain the benefits of the laws of another jurisdiction . . . .'" Id. (quoting Van Dusen v. Barrack, 376 U.S. 612, 639 (1964)). The exception does not apply when transfer was necessitated by a forum-selection clause, which is not the case here. See id.

Defendants have relied on both California and New York law, and urge that the Court need not resolve any choice-of-law questions because the Complaint fails to state a claim under either jurisdiction. Rudolph urges that California law applies, but argues that she has stated claims for relief under the laws of either state. (Opp. Mem. at 12 n.7.)

California "has applied the so-called governmental interest analysis in resolving choice-of-law issues." Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 107 (2006). This three-step analysis looks to whether 1.) the laws of the relevant jurisdictions are the same or different, 2.) considers each jurisdiction's interest in the application of its own laws to determine "whether a true conflict exists," and 3.) compares each jurisdictions interest in the application of its own law "to determine which state's interest would be more impaired if its policy were subordinated to the policy of the other state." Id. at 107-08 (quotation marks omitted).

As will be noted, for each of Rudolph's common law claims, the laws of California and New York are substantially the same. The Court therefore need not proceed past the first step of Kearny in the choice-of-law analysis.

C. The Complaint Adequately States a Claim for Negligence.

"Under New York law, in order to recover on a claim for negligence, a plaintiff must show '(1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof.'" Caronia v. Philip Morris USA, Inc., 715 F.3d 417, 428 (2d Cir. 2013) (quoting Akins v. Glens Falls City School Dist., 53 N.Y.2d 325, 333 (1981)). California has the same elements. Peredia v. HR Mobile Servs., Inc., 25 Cal. App. 5th 680, 687 (Cal. Ct. App. 2018) ("The elements of any negligence cause of action are duty, breach of duty, proximate cause, and damages.").

Defendants urge that the Complaint does not plausibly allege negligence because Rudolph has not demonstrated an injury, including out-of-pocket loss. However, for the reasons discussed, the Court concludes that Rudolph has identified loss based on the expense she incurred when she drove to a Bank of America branch to obtain a new debit card, as well as time expended to retrieve the card and update account records. This is sufficient to allege injury. See, e.g., Walters v. Kimpton Hotel & Rest. Grp., LLC, 2017 WL 1398660, at *2 (N.D. Cal. Apr. 13, 2017); Sackin, 278 F. Supp. 3d at 749.

Separately, defendants' argument that the losses she accrued to secure a replacement card "too attenuated to be attributable to the payment card incident" (Def. Mem. at 13) is more appropriately addressed at summary judgment or at trial.

Defendants' argument that Rudolph's claim is barred by the economic loss doctrine is also misplaced. In some circumstances, such as a construction accident that causes

widespread damage and disruption, New York courts have engaged in "[p]olicy-driven line-drawing" to conclude that defendants owed a duty "to those who have . . . suffered personal injury or property damage," and not to those who suffered an "economic loss alone . . . ." 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 96 N.Y.2d 280, 292 (2001); see also Ambac Assurance Corp. v. U.S. Bank Nat'l Ass'n, 328 F. Supp. 3d 141, 159 (S.D.N.Y. 2018) (the "applicability of the economic loss rule outside the product-liability context from which it originated is doubtful.") (Pauley, J.). Defendants have not explained how such a limitation on negligence liability could apply to the data breach alleged in this case. See Sackin, 278 F. Supp. 3d at 749-50 (declining to apply economic loss rule to data breach claim).

Defendants' motion to dismiss the negligence claim is therefore denied.

D. The Claim for Negligence *Per Se* Is Dismissed.

Under New York law, "violation of a State statute that imposes a specific duty constitutes negligence per se, or may even create absolute liability." Elliott v. City of New York, 95 N.Y.2d 730, 734 (2001). California law similarly "provides that negligence of a person is presumed if he violated a statute or regulation of a public entity, if the injury resulted from an occurrence that the regulation was designed to prevent, and if the person injured was within the class for whose protection the regulation was adopted." Elsworth v. Beech Aircraft Corp., 37 Cal 3d. 540, 544-45 (1984).

The Complaint does not allege the violation of a New York statute, but it does assert a violation of California's Consumer Records Act and its unfair competition law. But under California law, negligence per se "is an evidentiary doctrine" that establishes a rebuttable presumption of negligence if certain elements are proved. Quiroz v. Seventh Ave. Ctr., 140 Cal.

App. 4th 1256, 1285 (Cal. Ct. App. 2006). "[T]o apply negligence per se is not to state an independent cause of action." Id.

Rudolph appears to acknowledge that California does not recognize a claim of negligence per se, and "requests this Court construe Plaintiff's negligence per se claim as a traditional negligence claim, but apply the negligence per se doctrine." (Opp. Mem. at 16.)

Rudolph's negligence per se claim is dismissed because it is encompassed by her negligence claim. Any application of the negligence per se presumption is more properly raised at summary judgment or trial.

E. The Complaint Adequately Alleges Breach of an Implied Contract .

The Complaint asserts that defendants breached an implied contract with Rudolph by failing to safeguard her payment-card data. (Compl't ¶¶ 117-23.) Under California law, "an implied contract is an agreement, the existence and terms of which are manifested by conduct . . . ." Pacific Bay Recovery, Inc. v. California Physicians' Servs., Inc., 12 Cal. App. 5th 200, 215 (Cal. Ct. App. 2017); see also Cal. Civil Code § 1621 ("An implied contract is one, the existence and terms of which are manifested by conduct."). An implied contract is formed through the same elements as an express contract: offer, acceptance and consideration. Pacific Bay, 12 Cal. App. 5th at 215. New York law is similar. See, e.g., Maas v. Cornell Univ., 94 N.Y.2d 87, 94 (1999) (an implied contract may be inferred by conduct that demonstrates "such elements as consideration, mutual assent, legal capacity and legal subject matter.").

According to Rudolph, when she used her debit card at Saks OFF 5TH, she "entered into [an] implied contract[] with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of [her] Customer Data." (Compl't ¶ 119.) She states that defendants solicited her to shop at Saks OFF 5TH and

make purchases with her credit or debit card, and that she "accepted" the "offer." (Compl't ¶ 118.) In using her debit card, she contends that she entered into an implied contract whereby defendants agreed to protect her card information. (Compl't ¶ 119.) She alleges that defendants breached the contract by not protecting that data or detecting the breach within a reasonable time. (Compl't ¶ 122.)

Rudolph also points to a privacy policy published by Saks OFF 5TH prior to the breach, which told customers that "[o]nce we receive your transmission, we will take reasonable precautions to secure and protect the information on our systems." (Compl't ¶ 65.) After the data breach, the policy was revised to state that "we cannot guarantee our security measures," despite "every effort to help ensure the integrity and security of our network and systems . . . ." (Compl't ¶ 65.)

Defendants argue that "[a] promise to perform a preexisting legal duty is not supported by consideration." U.S. Ecology, Inc. v. State of California, 92 Cal. App. 4th 113, 129 (Cal. Ct. App. 2001). In U.S. Ecology, the parties' express contract contained a promise that the plaintiff would maintain a project schedule or else be subject to forfeiture of a performance bond. Id. However, a governing regulation contained language "identical" to the parties' agreement. Id. The court concluded that plaintiffs' promise to maintain the schedule, under penalty of bond forfeiture, "did not create contractual duties" and therefore did not amount to consideration. Id. The defendants here urge that because California statute creates a legal duty to maintain data security, plaintiffs cannot demonstrate consideration on the part of defendants. See Cal. Civil Code § 1798.81.5(b) ("A business that . . . maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate

to the nature of the information, to protect the personal information from unauthorized access . . . or disclosure.").

Other courts applying California law have concluded that an implied contract is formed where a person discloses sensitive information in order to receive a benefit, with the expectation that such information will be protected. Castillo v. Seagate Tech., LLC, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016) ("[I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."); Walters, 2017 WL 1398660, at *2 (plaintiff alleged an implied contract by which defendant agreed to safeguard payment-card information, based in part on a published privacy policy stating that defendant was "committed" to safeguarding personal information). These decisions did not address whether section 1798.81.5(b) had already created such a statutory duty on the part of the defendant.

At the motion to dismiss stage, drawing ever reasonable inference in favor of Rudolph, the Court concludes that the Complaint plausibly alleges the existence of an implied contract, including the element of consideration. At the pleading stage, the Court is unable to discern the extent to which California's data-protection statute overlaps with any implied promise to maintain data customers' protection. This action is thus unlike U.S. Ecology, where the language of an express agreement was "identical" to a regulation. 92 Cal. App. 4th at 129. The Complaint adequately alleges that defendants promised to safeguard payment-card information in exchange for a customer's payment, as indicated both by conduct and published statements by Saks OFF 5TH. (Compl't ¶¶ 65, 118-19.)

Defendants' motion to dismiss the claim for breach of implied contract is therefore denied.

F. Rudolph's Complaint States a Claim for Unjust Enrichment.

The Complaint alleges that Rudolph conferred a monetary benefit to defendants when she purchased items at Saks OFF 5TH and provided the store with her payment information. (Compl't ¶ 171.) It alleges that defendants failed to provide her full compensation in exchange for her payment data, which they acquired "through inequitable means" because they failed to disclose "inadequate security practices . . . ." (Compl't ¶¶ 173-74.) The Complaint alleges that "it would be unjust" to permit defendants to retain any benefits conferred by Rudolph and others, and that defendants' proceeds on the transaction should be disgorged. (Compl't ¶¶ 177-78.)

Under California law, "[t]he elements of an unjust enrichment claim are the receipt of a benefit and the unjust retention of the benefit at the expense of another." Peterson v. Cellco P'ship, 164 Cal. App. 4th 1583, 1593 (Cal. Ct. App. 2008) (quotation marks and alteration omitted). New York law is similar. Georgia Malone & Co. v. Ralph Rieder, 86 A.D.3d 406, 411 (1st Dep't 2011) ("It is well established that to successfully plead unjust enrichment a plaintiff must show that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered.") (quotation marks and alteration omitted).

Courts have concluded that the failure to secure a plaintiff's data can give rise to an unjust enrichment claim. They reason that a defendant has accepted the benefits accompanying plaintiff's data, but does so at the plaintiff's expense by not implementing adequate safeguards, thus making it "inequitable and unconscionable" to permit defendant to

retain funds that it saved by "shirking data-security" and leaving the plaintiff "to suffer the consequences." Sackin, 278 F. Supp. 3d at 751; see also In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) ("If Plaintiffs can establish that they shopped at Target after Target knew or should have known of the breach, and that Plaintiffs would not have shopped at Target had they known about the breach, a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target 'in equity and good conscience' should not have received.").

Here, Rudolph has plausibly alleged: (a) that she purchased merchandise from Saks using her Bank of America debit card, (b) that she would not have purchased the merchandise if Saks had not accepted the debit card, and (c) that the purchase of merchandise conferred a benefit on Saks and Hudson's. (Compl't ¶¶ 171, 172, 175.) Defendants urge that Rudolph has not stated a claim for unjust enrichment because she does not allege that the items she acquired at Saks were defective or worth less in value than the price she paid. (Def. Mem. at 17-18.) But her unjust enrichment claim is not directed to the value of the goods received. Rather, she asserts that the defendants profited from her purchase but by failing to secure her card data, they "did not provide full compensation for the benefit [the data] provided." (Compl't ¶¶ 172-73.) Rudolph alleges that it would be "unjust" for defendants "to retain" any benefit she conferred. (Compl't ¶ 177.)

The Court concludes that Rudolph has adequately alleged a claim for unjust enrichment, consistent with Sackin and Target. She has alleged that defendants benefitted from her use of a debit card, and have wrongfully retained the benefits of that transaction despite failing to secure her data.

To the extent that defendants urge the claim should be dismissed because it is duplicative of Rudolph's claim for breach of implied contract, where the existence and terms of a contract are in dispute, a claim premised on unjust enrichment may proceed in the alternative. See, e.g., Raisin Bargaining Ass'n v. Hartford Cas. Ins. Co., 2010 WL 3783871, at *3 (E.D. Cal. Sept. 27, 2010) ("Although a quasi-contract action cannot lie where there exists between the parties a valid express contract covering the same subject matter, quasi-contract actions may be utilized to prevent unjust enrichment regarding disputes between contracting parties that are related to, but outside the scope of, the parties' contract.") (applying California law); Fed. Deposit Ins. Corp. v. Dintino, 167 Cal. App. 4th 333, 346 (Cal. Ct. App. 2008) ("[A] cause of action for unjust enrichment is not based on, and does not otherwise arise out of, a written contract. Rather, unjust enrichment is a common law obligation implied by law based on the equities of a particular case and not on any contractual obligation."); Leroy Callender, P.C. v. Fieldman, 252 A.D.2d 468, 469 (1st Dep't 1998) ("where there is a bona fide dispute as to the existence of a contract or where the contract does not cover the dispute in issue, plaintiff may proceed upon a theory of quantum meruit and will not be required to elect his or her remedies.") (quotation marks omitted).

Defendants' motion to dismiss the claim for unjust enrichment is therefore denied.

G. Rudolph's Claim Under the Mississippi Consumer Protection Act Is Dismissed.

Rudolph brings a claim under the Mississippi Consumer Protection Act, Mississippi Code § 75-24-5(2) ("MCPA"). (Compl't ¶¶ 202-14.) She alleges that defendants engaged in unfair and deceptive trade practices by failing to implement adequate security measures, thereby misrepresenting the quality of their goods and services. (Id.) The Complaint

premises its Mississippi claim on the assertion that defendants maintain a "support operation center" in Mississippi, which tracks every POS transaction for Saks OFF 5TH. (Compl't ¶ 31.)

The MCPA requires that before a private action may be brought, "the plaintiff must have first made a reasonable attempt to resolve any claim through an informal dispute settlement program approved by the Attorney General." Miss. Code § 75-24-15(2). "Mississippi law is clear that 'failure to satisfy the prerequisite of an attempt at informal dispute resolution is fatal to a MCPA claim.'" Humphrey v. Citibank NA, 2013 WL 5407195, at *6 (N.D. Miss. Sept. 25, 2013) (quoting Wilson v. New Palace Casino, L.L.C., 2013 WL 870350, at *12 (S.D. Miss. Mar. 7, 2013)); accord Taylor v. S. Farm Bureau Cas. Co., 954 So. 2d 1045, 1049 (Miss. Ct. App. 2007) ("The record in this case is devoid of any reference to [plaintiff] attempting to resolve this issue through an informal settlement program, and we can only conclude that no such attempt was made. Therefore . . . the decision of the lower court to dismiss the action would still have been proper.").

Rudolph does not contend that she engaged in the dispute-resolution process required by the MCPA, and argues that any requirement that she do so amounts to a heightened pleading standard inconsistent with Rule 8. (Opp. Mem. at 21.) But the requirement that a plaintiff exhaust or grieve a statutory claim before bringing a private action is not novel and can be satisfied with notice pleading. See, e.g., Deravin v. Kerik, 335 F.3d 195, 200-01 (2d Cir. 2003) (summarizing exhaustion prerequisite to Title VII claims).

Because Rudolph has not alleged that she engaged in the mandatory dispute-resolution process prior to bringing her MCPA claim, the claim is dismissed.

H. Rudolph's Claim Under the California Customer Records Act Is Dismissed in Part.

Rudolph brings a claim under the California Customer Records Act, California Civil Code §§ 1798.81.5 and 1798.82 ("CRA"). (Compl't ¶¶ 146-55.) It alleges that defendants violated the CRA in two respects. First, they allegedly breached section 1798.81.5 by "failing to implement adequate and reasonable data security measures . . . ." (Compl't ¶ 151.) Second, they allegedly breached section 1798.82 by failing to provide adequate written notice of the breach. (Compl't ¶ 154.)

The CRA provides in part that a "business that owns, licenses or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access . . . or disclosure." Cal. Civ. Code § 1798.81.5(b). "Personal information" is defined to include a person's name "in combination with . . . credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Id. § 1798.81.5(d)(1)(A)(iii).

The CRA also requires that a California business must disclose any breach of "unencrypted personal information . . . acquired by an unauthorized person . . . ." Id. § 1798.82(a). Notice must be provided in written form and in a prescribed format, including certain specified headings and explanations "written in plain language." Id. § 1798.82(d)(1). According to Rudolph, defendants have not provided the notice required by section 1798.82, and are in continuing violation of that provision of the CRA. (Compl't ¶¶ 154-55.)

1. The Complaint Alleges Statutory Injury under the CRA.

Defendants urge that the CRA claim should be dismissed because Rudolph has not alleged an injury sufficient to confer Article III standing. However, for the reasons explained, the Court concludes that Rudolph has adequately identified an injury-in-fact, which is sufficient to establish an injury under the CRA. See, e.g., In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1218 (N.D. Cal. 2014) ("Although Section 1798.84 does not define what qualifies as an injury under the statute, other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact standard suffices to establish statutory injury under the CRA.").

2. The Complaint Fails to Allege Deficient Notice under Section 1798.82.

Defendants separately urge that to the extent the CRA claim is premised on failure to publish an adequate breach notice, it should be dismissed. They urge that providing notice through a website is adequate notice. Cal. Civ. Code § 1798.82(j)(3)(B) ("[s]ubstitute notice" may be made with a "[c]onspicuous" notice published on the affected business's website for at least 30 days). They note that the Complaint references a disclosure of the data breach made by the retailers' websites, including the site of Saks OFF 5TH. (Compl't ¶ 80.)

In opposition, Rudolph notes that her claim is not premised on the mere absence of notice, but asserts that defendants' notice failed to comply with the specific requirements prescribed by the CRA. But the Complaint does not identify what categories of information were omitted from defendants' online notice or how the notice failed to satisfy the CRA. The statute provides in part:

> The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved,"

> "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

Cal. Civil Code § 1798.82(d)(1). It proceeds to prescribe the minimum font size for the notice, require that the title and heading be "conspicuously displayed," and require that "[t]he format of the notice shall be designed to call attention to the nature and significance of the information it contains." Id.

The Complaint fails to plausibly allege any deficiency in the defendants' notice. Further, on a motion to dismiss, the Court may look to any document that is integral to the Complaint or incorporated by reference without converting the motion into one for summary judgment. See, e.g., Sierra Club v. Con-Strux, LLC, 911 F.3d 85, 88 (2d Cir. 2018). The form of notice submitted by defendants includes the headings required by the CRA, and Rudolph has not alleged any infirmities in its contents. (Schachter Reply Dec. Ex. 1.)

Because the Complaint does not identify any deficiency in the breach notice that defendants published online, Rudolph's CRA claim is dismissed to the extent that it is premised on a failure to provide notice.

I. The Motion to Dismiss Rudolph's Claim under California Unfair Competition Law Is Denied.

The Complaint brings a claim under California's Unfair Competition Law ("UCL"), California Business & Professions Code §§ 17200, et seq. (Compl't ¶¶ 191-201.) Defendants urge that the claim should be dismissed because Rudolph does not adequately allege an economic injury, which is narrower category than Article III standing and requires "injury in fact," including "lost money or property as a result of the unfair competition." Graham v. VCA Animal Hosp., Inc., 729 Fed. App'x 537, 539 (9th Cir. 2017) (summary order).

The California Supreme Court has stated that "[t]here are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." Kwikset Corp. v. Superior Court, 51 Cal. 4th 310, 323 (2011). An allegation that a plaintiff has "lost money and time" as a result of a defendant's UCL violation is sufficient to identify injury under the statute. Hameed-Bolden v. Forever 21 Retail, Inc., 2018 WL 6802818, at *4 (C.D. Cal. Oct. 1, 2018).

Because the Complaint has identified injury based on the time and expense that Rudolph incurred as a result of the alleged data breach, she has adequately alleged injury under the UCL. The motion to dismiss her UCL claim is therefore denied.

J. The Declaratory Judgment Act Claim Is Dismissed.

The Complaint brings a claim under the Declaratory Judgment Act, 28 U.S.C. § 2201. (Compl't ¶¶ 179-90.) It seeks various declarations related to defendants' contractual obligations and their duty of care as to customer information. Because the relief sought is duplicative of Rudolph's claims for negligence and breach of contract, her claim under the Declaratory Judgment Act is dismissed. See, e.g., Amusement Indus., Inc. v. Stern, 693 F. Supp. 2d 301, 311 (S.D.N.Y. 2010) ("The fact that a lawsuit has been filed that will necessarily settle the issues for which the declaratory judgment is sought suggests that the declaratory judgment will serve 'no useful purpose.'") (Kaplan, J.) (collecting cases).

CONCLUSION.

Defendants' motion to dismiss the Complaint pursuant to Rule 12(b)(1) is denied as to the time and expense that arose when plaintiff obtained a new debit card but granted as to any claim premised on future injury.

Defendants' motion to dismiss the Complaint pursuant to Rule 12(b)(6) is granted as to Rudolph's claim for negligence per se, her claim under the Declaratory Judgment Act, her claim under Mississippi's consumer-protection statute, and her notice-based claim under California's Customer Records Act. It is denied as to her common law claims of negligence, breach of contract and unjust enrichment, her claim under California's Unfair Competition Law, and her claim that defendants did not implement reasonable data-security procedures under the California Customer Records Act.

The Clerk is directed to terminate the motion. (Docket # 80.)

SO ORDERED.

P. Kevin Castel
United States District Judge

Dated: New York, New York
May 7, 2019