UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOEL RUIZ, on behalf of himself and all others similarly situated, Plaintiff, v. GAP, INC., and VANGENT, INC., Defendants.	Case No. 07-5739 SC ORDER GRANTING DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT

I. INTRODUCTION

On February 13, 2009, Defendant Vangent, Inc. ("Vangent") filed a Motion for Summary Judgment. Docket No. 99 ("Vangent's Motion"). On the same day, Defendant Gap, Inc. ("Gap") filed a Motion for Summary Judgment. Docket No. 100 ("Gap's Motion"). On February 27, 2009, Plaintiff Joel Ruiz ("Plaintiff" or "Ruiz") filed an Opposition. Docket No. 104. On March 6, 2009, Gap submitted a Reply, and Vangent submitted a Reply. Docket Nos. 112, 116. For the reasons stated herein, Vangent's Motion is GRANTED and Gap's Motion is GRANTED.

Various other motions have been filed, including Plaintiff's Motion for Class Certification, Gap's Request for Judicial Notice, Plaintiff's Request for Judicial Notice, and Defendants' Motion to Strike and Objections to Plaintiff's Expert Reports. See Docket Nos. 92, 102, 106, 114. Defendants filed a Joint Opposition to

Plaintiff's Request for Judicial Notice. Docket No. 115. The Court granted Plaintiff leave to file an Opposition to Defendants' Motion to Strike, and Plaintiff did so on March 16, 2009. See Docket Nos. 120, 121. The Court GRANTS Gap's Request for Judicial Notice, and the Court GRANTS Plaintiff's Request for Judicial Notice. The Court DENIES Defendants' Motion to Strike and Objections to Plaintiff's Expert Reports.

II. BACKGROUND

A. Factual Background

On September 17, 2007, a thief gained entry to Vangent's offices in Chicago, Illinois, and stole two laptop computers. Docket No. 89 ("Am. Compl.") ¶ 6. Vangent, a Gap vendor, processes Gap job applications. Id. ¶ 3. At the time the laptop computers were stolen, one of the computers was downloading information about Gap job applicants. Id. ¶ 40. A Vangent employee intended to use the information to prepare a report on Gap's geographic hiring trends. Id. At the time it was stolen, the laptop computer contained the personal information, including social security numbers, of approximately 750,000 Gap job applicants. Id. ¶ 6. The information was not encrypted. Id. ¶ 7.

On September 28, 2007, Gap sent a notification letter to the applicants whose personal information was on the computer. See Stern Decl. Ex. C ("Notification Letter").[1] Ruiz received the

[1] William L. Stern, counsel for Gap, filed a declaration in support of Gap's Motion. Docket No. 101.

letter in early October 2007. Stern Decl. Ex A ("Ruiz Dep.") at 25:9-24. Gap offered to provide these applicants with twelve months of credit monitoring with fraud assistance at no cost. See Notification Letter. Gap advised job applicants to notify their banks and sign up for a free credit report from one of the three major credit reporting agencies. See id. Ruiz did not enroll for the free credit monitoring. Stern Decl. Ex A ("Ruiz Dep.") at 32:3-25. Ruiz did not contact his bank, and although he attempted to sign up for a free credit report, he thinks he was unsuccessful. See id. at 37:20-39:16.

B. Procedural Background

On November 13, 2007, Ruiz filed a Complaint asserting the following causes of action: (1) negligence; (2) bailment (3) violation of California Business and Professions Code § 17200 et seq.; (4) violation of the California Constitutional right to privacy; and (5) violation of California Civil Code § 1798.85. See Docket No. 1 ("Compl."). On March 24, 2008, the Court granted judgment on the pleadings in favor of Gap on the second, third, and fourth claims. See Docket No. 46 ("March 24 Order"). On October 2, 2008, the Court denied Gap's Motion to Strike Plaintiff's Class Definition. See Docket No. 75 ("October 2 Order"). Although originally set for October 1, 2008, the discovery cutoff was extended to December 23, 2008. Id. at 1-2. On February 9, 2009, Plaintiff filed an Amended Complaint naming Vangent as a defendant and adding a breach of contract claim against Vangent. See Am. Compl.

III. LEGAL STANDARD

Entry of summary judgment is proper "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "Summary judgment should be granted where the evidence is such that it would require a directed verdict for the moving party." Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 250 (1986). Thus, "Rule 56(c) mandates the entry of summary judgment . . . against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986). In addition, entry of summary judgment in a party's favor is appropriate when there are no material issues of fact as to the essential elements of the party's claim. Anderson, 477 U.S. at 247-49.

IV. DISCUSSION

A. Standing

As a threshold matter, the Court determines whether Ruiz has standing to bring this suit. To satisfy the standing requirement of Article III of the Constitution, there must be the "irreducible constitutional minimum" of an injury-in-fact. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). An injury-in-fact is "an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural

or hypothetical." Id. (internal citations and quotation marks omitted).

Some courts have held that plaintiffs in "lost-data" cases have not suffered an injury-in-fact sufficient to confer Article III standing. See Randolph v. ING Life Ins. and Annuity Co., 486 F. Supp. 2d 1, 6-8 (D.D.C. 2007) (no standing where laptop computer stolen during burglary and plaintiffs pled increased risk of identity theft); Bell v. Axiom Corp., No. 06-0485, 2006 WL 2850042, at *1-2 (E.D. Ark. Oct. 3, 2006) (class action dismissed for lack of standing where hacker downloaded information and sold it to marketing company); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (class action dismissed for lack of standing where unauthorized persons obtained access to information of approximately 96,000 customers); Giordano v. Wachovia Sec. LLC, No. 06-476, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006) (credit monitoring costs resulting from lost financial information did not constitute injury sufficient to give plaintiff standing).

However, the only circuit court to consider the question of standing in a lost-data case determined that the plaintiff did have standing to assert negligence and contract claims. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007). Old National Bancorp ("ONB") operated a marketing website where individuals seeking banking services could complete online applications. Id. at 631. The applications requested names, addresses, social security numbers, driver's license numbers, date of birth, mother's maiden name, and other information. Id. A third-party hacker obtained access to the information of tens of

thousands of applicants. Id. The scope and manner of access suggested the intrusion was "sophisticated, intentional and malicious." Id. at 632. After ONB sent written notice to those affected, plaintiffs filed a putative class action asserting negligence and breach of contract claims and requesting compensation for credit monitoring services. Id. The Seventh Circuit held that plaintiffs had standing because "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." Id. at 634.

Relying on Pisciotta, the District Court for the Southern District of New York determined that plaintiffs had standing in a lost-data case. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 280 (S.D.N.Y. 2008). In Caudle, an employee was notified that several laptop computers had been stolen, one of which contained the employee's personal information, including his social security number. Id. at 276. Although the Second Circuit has not decided whether the standing requirement can be satisfied by an increased future risk of identity theft, the Second Circuit has decided that standing exists where there is an increased future risk of harm based on exposure to environmental toxins or potentially unsafe food products. See Baur v. Veneman, 352 F.3d 625, 634 (2d Cir. 2003); LaFleur v. Whitman, 300 F.3d 256, 270 (2d Cir. 2002). Against this backdrop, the court determined the plaintiff alleged an adequate injury-in-fact for standing purposes. Caudle, 580 F. Supp. at 280.

The Court finds that Ruiz has standing to bring this suit. Like the plaintiffs in Pisciotta, Ruiz submitted an online application that required him to enter his personal information, including his social security number. See Am. Comp. ¶ 38. Like the theft in Caudle, this theft involves laptop computers that contained personal information. See id. ¶ 46. Here, it is less clear than it was in Pisciotta that the thief was targeting the plaintiff's personal information. Ruiz submits the expert opinion of Dr. Larry Ponemon to support this contention. Rivas Decl., Ex. N ("Ponemon Decl.").[2] Dr. Ponemon opines that given the nature of the theft, "it is substantially likely that the laptops were stolen for the Gap employee applicant data." Id. ¶ 2. This opinion conflicts with that of the Chicago Police Department and the Federal Bureau of Investigation ("FBI"), who viewed the theft as a property crime, where the thief was after the laptop computers themselves, rather than the information they contained. Stern Decl. Ex. B ("White Dep.") at 89:21-23; 125:3-9. However, in Caudle, the court determined that the plaintiff had standing even though nothing in the record shed light on "whether the laptops were stolen for their intrinsic value, for the value of the data or for both." 580 F. Supp. 2d at 276.

While the Ninth Circuit has not determined that standing exists based on an increased risk of identity theft, it has determined in a case concerning the management of water resources

[2] Rosemary M. Rivas, counsel for Ruiz, submitted a declaration in opposition to Defendants' motions for summary judgment. Docket No. 105.

that "the possibility of future injury may be sufficient to confer standing . . ." Cent. Delta Water Agency v. United States, 306 F.3d 938, 947 (9th Cir. 2002). Furthermore, Ruiz submits an expert report in support of his contention that he faces an increased risk of identity theft. Rivas Decl. Ex. M ("Van Dyke Decl."). According to a study conducted by James Van Dyke in 2008, "of the 11% of Americans notified of a data breach in the last 12 months, 19% reported becoming victims of identity fraud in the last 12 months. In contrast, only 4.32% of all Americans reported becoming victims of identity fraud in the last 12 months, a difference reflecting over a four-to-one general increased likelihood that a data breach will lead to actual fraud victimization." Id. ¶ 4. Based on Ruiz's increased risk of identity theft, and the reasoning of several federal courts including the Seventh Circuit, the Court finds that Ruiz has standing to bring this suit.

B. Ruiz's Negligence Claim

Ruiz alleges that as a result of Defendants' failure to exercise due care, "Plaintiff and the Class have been injured and harmed since Defendants' compromising of their [personal information] has placed them at an increased risk of identity theft. Plaintiff and the Class have suffered damages; they have spent and will continue to spend time and/or money in the future to protect themselves as a result of Defendants' conduct." Am. Compl. ¶ 80.

Under California law, appreciable, nonspeculative, present harm is an essential element of a negligence cause of action. Aas

v. Super. Ct., 24 Cal. 4th 627, 646 (2000). Under California law, the breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence. See id.; see also Zamora v. Shell Oil Co., 55 Cal. App. 4th 204, 211 (4th Dist. 1997) (finding there has not been the requisite damage for a negligence cause of action where defective water pipes had not yet leaked); San Francisco Unified Sch. Dist. v. W.R. Grace & Co. 37 Cal. App. 4th 1318, 1327-30 (1st Dist. 1995) (finding that presence of asbestos products in buildings did not satisfy damage element of negligence cause of action when products had not contaminated buildings by releasing friable asbestos); Khan v. Shiley, Inc., 217 Cal. App. 3d 848, 857 (4th Dist. 1990) (no cause of action for negligence premised on risk that implanted heart valve may malfunction in the future).

While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law. Ruiz testified that he has never been a victim of identity theft. See Ruiz Dep. at 23:17-19; 73:10-12. Ruiz's case hinges on his increased risk of future identity theft. To support his contention that this risk is sufficient to assert a negligence claim, Ruiz relies on cases where California courts allowed recovery for future medical monitoring after the plaintiffs were exposed to toxic substances. See In re Mattel, Inc., 588 F. Supp. 2d 1111, 1116-17 (C.D. Cal. 2008); Potter v. Firestone Tire & Rubber Co., 6 Cal. 4th 965, 1009 (1993).

Ruiz's reliance on these medical monitoring cases is

misplaced for a number of reasons. First, Ruiz has not presented any authority that endorses treating lost-data cases as analogous to medical monitoring cases. This Court doubts a California court would view these two types of cases as analogous. For example, in allowing recovery of medical monitoring costs, the California Supreme Court in Potter noted that "there is an important public health interest in fostering access to medical testing for individuals whose exposure to toxic chemicals creates an enhanced risk of disease, particularly in light of the value of early diagnosis and treatment for many cancer patients." 6 Cal. 4th at 1008. There is no such public health interest at stake in lost-data cases.

Second, even if a California court were to treat these kinds of cases as analogous, the Court notes that toxic exposure plaintiffs seeking to recover the costs of future medical monitoring face "significant evidentiary burdens." Id. at 1009. In Potter, the court held that:

> the cost of medical monitoring is a compensable item of damages where the proofs demonstrate, through reliable medical expert testimony, that the need for future monitoring is a reasonably certain consequence of a plaintiff's toxic exposure and that the recommended monitoring is reasonable. In determining the reasonableness and necessity of monitoring, the following factors are relevant: (1) the significance and extent of the plaintiff's exposure to chemicals; (2) the toxicity of the chemicals; (3) the relative increase in the chance of onset of disease in the exposed plaintiff as a result of the exposure, when compared to (a) the plaintiff's chances of developing the disease had he or she not been exposed, and (b) the chances of the members of the public at large of developing the disease; (4) the seriousness of

> the disease for which the plaintiff is at risk; and (5) the clinical value of early detection and diagnosis.

Id. Ruiz has not presented evidence sufficient to overcome the kind of evidentiary burdens that apply in medical monitoring cases. At a minimum, Ruiz would be required to present evidence establishing a significant exposure of his personal information. Here, Ruiz has not presented such evidence. Instead, Ruiz relies on the expert report of Dr. Ponemon to overcome this evidentiary burden. See Opp'n at 11. However, as Ruiz himself concedes, all Dr. Ponemon's report establishes is that there is a "significant risk" that Ruiz's information was exposed. See id. Ruiz presents no evidence showing there was an actual exposure of his personal information, much less that it was significant and extensive. The Court is convinced that even if a California court were to apply the standard it has adopted in medical monitoring cases, summary adjudication of Ruiz's negligence claim would still be appropriate.

In an unpublished decision, the Ninth Circuit made a similar determination when considering Arizona law. See Stollenwerk v. Tri-West Health Care Alliance, 254 Fed. Appx. 664, 665-67 (9th Cir. 2007). Plaintiffs sued for negligence after Tri-West Health Care Alliance ("Tri-West") suffered a burglary and computer equipment containing their personal information was stolen. Id. at 665. The personal information included social security numbers. Id. Under Arizona law, toxic exposure plaintiffs can recover the costs of future medical monitoring by establishing a number of factors, including the significance and extent of

exposure. Id. at 666. Indeed, the standard for recovering medical monitoring costs under Arizona law is very similar to the standard under California law, as both standards are derived from the same New Jersey case, Ayers v. Township of Jackson, 106 N.J. 557 (1987). The Ninth Circuit determined that lost-data plaintiffs who presented no evidence of identity theft would not be able to meet Arizona's standard for recovery of monitoring costs. Stollenwerk, 254 Fed. Appx. at 667. Similarly, this Court is convinced that Ruiz cannot meet California's standard for recovery of monitoring costs because he has presented no evidence that there was a significant exposure of his personal information, and he has presented no evidence that he has become a victim of identity theft.

Furthermore, to the extent that Ruiz seeks to recover as damages the money he has spent monitoring his credit, Gap's letter notifying him of the theft of the laptop computers offered Ruiz one year of free credit monitoring and fraud insurance. See Notification Letter. Ruiz contends that credit monitoring beyond one year is reasonably necessary to minimize his risk of identity theft. See Opp'n at 6. The Court gives little weight to Ruiz contention because he chose not to take advantage of Gap's offer of one year of free credit monitoring. See Ruiz Dep. at 32:3-25.

This Court's determination with respect to Ruiz's negligence claim is consistent with those of other federal courts. In Pisciotta, as noted above, the Seventh Circuit determined that an online applicant whose personal information was compromised had standing to sue. 499 F.3d at 634. However, the Seventh Circuit

went on to determine that this compromise of the applicant's personal information did not rise to the level of a compensable injury and damages required to state a claim for negligence or for breach of contract under Indiana law. See id. at 635-39. The Seventh Circuit concluded that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy." Id. at 639. Similarly, in Caudle, where the court also found standing, the court went on to determine that a New York court would not allow a negligence claim to proceed in a case where "[d]espite a full and fair opportunity to conduct discovery, there is no evidence . . . regarding the motive or capabilities of the thief . . . [and] no evidence that this plaintiff's data has been accessed or used by anyone as a result of the theft." 580 F. Supp. 2d at 282.

In Melancon v. Louisiana Office of Student Financial Assistance, the court noted that "the mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence." 567 F. Supp. 2d 873, 877 (E.D. La. 2008)). In Kahle v. Litton Loan Servicing LP, computer equipment was stolen that contained the personal information of 229,501 former customers of Provident bank. 486 F. Supp. 2d 705, 706 (S.D. Ohio 2007). The court found that "without direct evidence that the information was accessed or specific evidence of identity fraud this Court can not find the cost of obtaining . . . credit monitoring to amount to damages in a negligence claim." Id. at 713.

In Forbes v. Wells Fargo Bank, N.A., computers were stolen

from a vendor of Wells Fargo Bank that contained unencrypted customer information. 420 F. Supp. 2d 1018, 1019 (D. Minn. 2006). The court granted summary judgment against the plaintiffs on their negligence claim because their expenditure of time and money monitoring their credit did not establish the essential element of damages. Id. at 1020-21. In Guin v. Brazos Higher Education Service Corp., a laptop computer was stolen that contained unencrypted, nonpublic customer information. No. 05-668, 2006 WL 288483, at *1 (D. Minn. Feb. 7, 2006). The court held that the plaintiff could not sustain a claim for negligence because he had experienced no instance of identity theft. Id. at *6.

Although these cases are not binding on this Court, the Court finds them persuasive. Plaintiff attempts to distinguish these cases by pointing out that they were not decided under California law. See Opp'n at 13-14. The Court notes, however, that the essential elements of a negligence claim are the same or similar in each of the other jurisdictions. Plaintiff also alleges that other Gap job applicants have claimed identity theft or have had their social security numbers used to open an account at T-Mobile. See Opp'n at 7. Ruiz, however, has presented no evidence in support of these allegations, so they are not sufficient to defeat a summary judgment motion. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248-49 (1986)(determining that nonmoving party must present significant probative evidence to defeat motion for summary judgment). The Court finds that Gap and Vangent are entitled to summary judgment on Ruiz's negligence claim.

///

C. Violation of California Civil Code Section 1798.85

California Civil Code § 1798.85 provides that a person or entity may not "[r]equire an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site." Cal. Civ. Code § 1798.85(a)(4). Ruiz alleges that Gap and Vangent violated this provision "[b]y requiring Plaintiff and Class Members to use SSNs to enter the application Web site without also requiring a unique personal identification number or other authentication device." Am. Compl. ¶ 82.[3]

The Court finds that Gap and Vangent did not require Ruiz to use his social security number to "access" the job application website. During his deposition, Ruiz reenacted Gap's online employment application process. See Ruiz Dep. at 52:23-59:7. Ruiz started from the Google website. Id. at 52:23-53:3. Ruiz entered a URL address which took him to the Gap website. Id. at 53:4-21. At this point in the application process, Ruiz had accessed the website. See Internet Specialties West, Inc. v. Milon-DiGiorgio Enters., Inc., 2009 WL 690302, at *9 (9th Cir. 2009)("A customer accesses ISPWest's website by entering the

[3] Ruiz's Opposition states that Plaintiff alleges only a violation of California Civil Code § 1798.85(a)(2). However, that provision states that a person or entity may not "[p]rint an individual's social security number on any card required for the individual to access products or services provided by the person or entity." Cal. Civ. Code § 1798.85(a)(2). The Court assumes that Ruiz intends to allege only a violation of California Civil Code § 1798.85(a)(4).

ISPWest domain name into their browser."). Ruiz was not required to enter his social security number to access the Gap website. Id. at 53:22-24. Ruiz navigated through several pages on the Gap website before he reached the page requiring him to enter his social security number. Id. at 53:25-59:7. While entering his social security number was required to submit his application, Gap and Vangent did not require Ruiz to use his social security number to access any website. Gap and Vangent are entitled to summary judgment on Ruiz's claim that there has been a violation of California Civil Code § 1798.85. The Court does not need to reach Gap and Vangent's contention that there is no private right of action under California Civil Code § 1798.85.

D. Ruiz's Breach of Contract Claim

Ruiz alleges a breach of contract claim against Vangent only. Am Compl. ¶¶ 84-91. Ruiz alleges that he and the putative class members are third-party beneficiaries of an Employment Screening Services Agreement ("Agreement") between Gap and Vangent. Id. ¶ 86. Ruiz alleges that Vangent breached the Agreement by, among other things, failing to employ commercially reasonable efforts to preserve the security and confidentiality of personal data under its control, and by failing to encrypt the data. Id. ¶ 89. Ruiz alleges that he and the putative class members "have been injured and harmed by Vangent's failure to comply with the terms of the Agreement. As a direct and proximate result of Vangent's breach, Plaintiff and the Class have suffered damages; they have spent time and/or money, and will continue to spend time and/or money in the future to protect themselves from harm." Id. ¶ 91.

Under California law, a breach of contract claim requires a showing of appreciable and actual damage. See St. Paul Fire and Marine Ins. Co. v. American Dynasty Surplus Lines Ins., 101 Cal. App. 4th 1038, 1060 (2d Dist. 2002) ("An essential element of a claim for breach of contract are damages resulting from the breach.")(italics omitted); Patent Scaffolding Co. v. William Simpson Const. Co., 256 Cal. App. 2d 506, 511 (2d Dist. 1967) ("A breach of contract without damage is not actionable."). Because Ruiz has not been a victim of identity theft, he can present no evidence of appreciable and actual damage as a result of the theft of the two laptop computers. In Aguilera v. Pirelli Armstrong Tire Corp., the Ninth Circuit determined that appellants could not show they were actually damaged by pointing to their "fear of future layoff." 223 F.3d 1010, 1015 (9th Cir. 2000). Similarly, this Court determines that Ruiz cannot show he was actually damaged by pointing to his fear of future identity theft.

Relying on Arcilla v. Adidas Promotional Retail Operations, Inc., 488 F. Supp. 2d 965, 972 (C.D. Cal. 2007), Ruiz asserts that "an increased risk of harm is compensable injury." Opp'n at 25. In Arcilla, the plaintiffs alleged that a retailer failed to truncate customers' credit card numbers and to obscure the expiration dates as required by the Fair Credit Transactions Act ("FCRA"). 488 F. Supp. 2d at 966. In denying the defendant's motion to dismiss, the court held that plaintiffs properly alleged actual harm in the form of heightened risk of identity theft. Id. at 967. In Arcilla, however, the court was construing the federal FCRA, not California contract law. Arcilla fails to support

Ruiz's contention that an increased risk of identity theft constitutes appreciable damage under California contract law.

Relying on Ross v. Frank W. Dunne Co., 119 Cal. App. 2d 690, 700 (1953), Ruiz asserts that "once a breach of contract has been proven nominal damages are presumed to follow as a conclusion of law." Opp'n at 24. In Aguilera, however, the Ninth Circuit noted that nominal damages, like speculative harm or fear of future harm, would not suffice to show legally cognizable damage under California contract law. 223 F.3d at 1015 (9th Cir. 2000)(quoting Buttram v. Owens-Corning Fiberglas Corp., 16 Cal. 4th 520, 531 n.4 (1997)).

Ruiz asserts that the costs he paid for credit monitoring are compensable because they constitute his attempt to mitigate damages. Ruiz relies on Brandon & Tibbs v. George Kevorkian Accountancy Corp., 226 Cal. App. 3d 442, 468 (5th Dist. 1990) to support this contention. In Brandon & Tibbs, the plaintiff sought to mitigate his lost profits damages by opening a new office when the defendant breached a joint venture agreement. See id. at 460-62. Here, however, Ruiz has no actual damages to mitigate since he has never been a victim of identity theft.

This decision is consistent with that of other federal courts considering breach of contract claims in lost-data cases. See Pisciotta, 499 F.3d at 633 (affirming district court's decision that "there could be no action for breach of contract under Indiana law in the absence of . . . cognizable damages"); Forbes, 420 F. Supp. 2d at 1021 (granting summary judgment in favor of defendant on lost-data plaintiff's breach of contract claim under

Minnesota law); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 779-80 (W.D. Mich. July 26, 2006) (dismissing contract claim of plaintiff who claimed as damages "the costs of protecting herself against a risk that the stolen data will, in the future, be used to her detriment" because plaintiff had "failed to allege damages of a type cognizable under Michigan common law applicable to contract actions."). Ruiz has presented no evidence of legally cognizable damage under California contract law, so Vangent is entitled to summary judgment on Ruiz's breach of contract claim. The Court does not need to reach Ruiz's argument that he and the putative class members are third party beneficiaries of the Agreement between Vangent and Gap.

V. CONCLUSION

For the reasons stated about, the Court GRANTS Gap's Motion for Summary Judgment and GRANTS Vangent's Motion for Summary Judgment. The Court DENIES Plaintiff's Motion for Class Certification as moot.

IT IS SO ORDERED.

Dated: April 6, 2009

UNITED STATES DISTRICT JUDGE