Justin F. Marquez (SBN 26417)
justin@wilshirelawfirm.com
Thiago M. Coelho (SBN 324715)
thiago@wilshirelawfirm.com
Robert J. Dart (SBN 264060)
rdart@wilshirelawfirm.com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

LAVARIOUS GARDINER, individually and on behalf of all others similarly situated, Plaintiff, v. WALMART, INC., a Delaware corporation; DOES 1 to 10, inclusive, Defendants.	Case No.: 4:20-cv-04618-JSW **PLAINTIFF LAVARIOUS GARDINER'S OPPOSITION TO DEFENDANT WALMART INC.'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT** Date: March 5, 2021 Time: 9:00 a.m. Courtroom: 5 Complaint filed: July 10, 2020 Trial date: Not set

TABLE OF CONTENTS

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF CONTENTS (continued)

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES

Cases **Page(s)**

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

TABLE OF AUTHORITIES (continued)

Codes	**Page(s)**
California Civil Code § 1798.81.5	21
California Civil Code § 1798.81.5(A)(1)(d)	7
California Civil Code § 1798.150	20
California Civil Code § 1798.150(a)(1)	5, 6, 7
California Civil Code § 3300	13
California Civil Code § 3333	12
California Civil Code § 3344.1	19

Rules	**Page(s)**
Federal Rules of Civil Procedure, Rule 8(a)(2)	4
Federal Rules of Civil Procedure, Rule 8(e)	7, 8
Federal Rules of Civil Procedure, Rule 12(b)(6)	4

Other Sources	**Page(s)**
3 Witkin, Cal. Procedure, Actions, § 139 (4th ed. 1996)	20
Federal Trade Commission Act, 15 U.S.C. § 45	21
Restatement (Second) of Torts § 919 (1979)	10

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendant Walmart, Inc. ("Walmart") failed to protect its customers' Private Identifiable Information ("PII"), including full names, addresses, and credit card and debit card information, and including all of the data necessary to access the credit card and debit card accounts. As a result of the data breach, over two-million Walmart accounts, including all of the information that customers provided to Walmart to create accounts and make purchases, are for sale on the dark web. There is a real and actual risk that criminals will purchase and have purchased this data on the dark web, creating real economic damage for Walmart's customers.

Walmart argues that it nonetheless cannot be held liable under the California Consumer Protection Act (CCPA) because Plaintiff Lavarious Gardiner has not alleged when specifically the data breach occurred, and has not alleged loss of "personal information" as defined in the Act. Walmart is wrong. Plaintiff has alleged that the disclosure—which, under the act, creates liability—is ongoing, as the data was, as of the time of the Complaint, still available on the dark web. That is all Plaintiff was required to allege with regard to timing. *See, e.g., Franco v. Grover*, No. CV-04-213-AHS SGL, 2005 WL 5955954, at *1 (C.D. Cal. Apr. 5, 2005) (rejecting defendant's argument that complaint was defective because it did not include specific dates when the alleged acts occurred). By alleging that the disclosure was ongoing, Plaintiff adequately placed Defendant on notice that it was liable under the CCPA. As to the loss of "personal information," Plaintiff has alleged the loss of credit card numbers and, by implication, the data necessary to access the card and the account, which is all that he was required to allege.

Walmart next argues that Plaintiff does not deserve compensation under any of his remaining causes of action because he cannot state appreciable, non-speculative harm as a result of the data breach. Walmart is wrong once again. Many courts have held that the element of damages was validly stated where a plaintiff alleged loss of value of the PII as harm, *see In re Facebook Privacy Litig.*, 572 Fed. Appx. 494 (9th Cir. 2014) —as Plaintiffs here allege—or lost time and money spent on credit monitoring, *see Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *4–5 (C.D. Cal. June 15, 2015)—as Plaintiff also

alleges. Plaintiff has also adequately pled injury by alleging that he is at a considerable risk of identity theft due to the breach. *In re Yahoo! Inc. Customer Data Security Breach Litigation*, 2017 WL 3727318 at *13 (N.D. Cal. 2017). Finally, Plaintiff has adequately pled an injury by alleging that he was denied the benefit of his bargain with Defendant, through which he contracted for minimum data protection standards which were not met. *In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783 at *13-14 (N.D. Cal. 2016) ("*Anthem II*")). Defendant cites other authority which rejected these theories where there was no actual risk of data theft involved. However, here, there is clearly such a risk. The data is for sale on the dark web. This isn't a case in which data was merely made publicly available, inadvertently, for a limited period of time, but a case in which the data has most definitely been stolen by hackers and is as of this minute being auctioned off to criminals. Clearly, a risk of fraud is present here.

Defendant points to the fact that Plaintiff has alleged both a hack of Defendant's systems and individual hacks of the Class Members' computers as a basis to deny liability. However, as is clear from examining Plaintiff's allegations as to the security vulnerabilities posed by Defendant's systems, certain website vulnerabilities, amounting to negligence on the part of Defendant, likely caused hacks of individual computers. As Defendant's negligence caused those hacks, Defendant is liable for them.

Defendant also argues that the economic loss doctrine bars recovery on Plaintiff's negligence claim. Defendant is wrong yet again. The economic loss doctrine does not apply for three reasons. First, Plaintiff has stated a duty of care based on statutory and regulatory guidelines which exists independently of the contract at issue. *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal.4th 979, 984 (2004); *Erlich v. Menezes*, 21 Cal. 4th 543, 551–52, 981 P.2d 978, 982–83 (1999). Second, Plaintiff has stated a non-economic harm resulting from the breach, namely, time spent monitoring credit. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019). Third, a special relationship exists between Plaintiff and Defendant because, among other factors, the harm to Plaintiff resulting from the data breach was highly foreseeable. *N. Am. Chem. Co. v. Superior Court*, 59 Cal. App. 4th 764, 777–87, 69 Cal. Rptr. 2d 466, 472–79 (1997). This is true whether or not contractual privity exists. *Stop Loss Ins. Brokers, Inc. v.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Brown & Toland Med. Grp., 143 Cal. App. 4th 1036, 1061, 49 Cal. Rptr. 3d 609, 629 (2006) ("[s]ubsequent cases have extended the application of *J'Aire* to cases where the parties are in contractual privity. [Citation.] ... [T]he reasoning of *J'Aire* is wholly incompatible with a limitation of the cause of action to those instances in which the plaintiff and defendant are not in privity.'") (quoting *North American Chemical Co. v. Superior Court* 59 Cal.App.4th 764, 783, 69 Cal.Rptr.2d 466, 476 (1997). When retailers fail to protect their customers' data, real harm results. That is why Plaintiff filed this lawsuit. Plaintiff's harms are compensable. His case should move forward, and Defendant's motion should be denied in its entirety.

II. PERTINENT FACTS

Defendant Walmart is a retailer selling goods at its stores and online via its website. (Complaint, ¶ 1.) Due to lax and insecure data protection methods, Walmart has suffered a data breach or data breaches resulting in over two million Walmart accounts being available for sale on the dark web. (*Id*., ¶ 15.) Aside from the fact that its accounts are available for sale on the dark web, evidence of a data breach can be found in the many vulnerabilities that Walmart's systems pose. (*Id*., ¶ 17.) A scan of Walmart's domains using Open Web Application Security Project Zed Attack Proxy ("OWASP ZAP"), which is widely used in the cybersecurity community to scan websites for documented vulnerabilities, resulted in the exposure of six major vulnerabilities. (*Id*.)

Scans using other highly respected vulnerability scanners resulted in affirmation of the aforementioned vulnerabilities, and the finding of additional vulnerabilities which hackers can take advantage of to obtain protected files from a website. (*Id*., ¶ 20.) For example, a scan of less than 2% of the Walmart website using the Vega vulnerability scanner uncovered 228 high ranked vulnerabilities. (*Id*.) These vulnerabilities include the integer overflow vulnerability, and numbers exposed which appeared to be social security numbers and credit card numbers. (*Id*.) Vega also found seven instances where local paths were revealed, which can allow hackers to obtain sensitive information about the server environment. (*Id*.) Other scans have revealed yet more paralyzing vulnerabilities. (*Id*., ¶¶ 21-24).

Walmart's system has been breached. (*Id*. ¶¶ 54-61.) It has failed to protect its

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

customers' data as required by the CCPA and other applicable law, and it must be held liable. (*Id*.) Walmart's contract with its customers included a Privacy Policy, which promised that Defendant would adopt reasonable security measures to protect the data in its possession, as follows:

> How Do We Secure Your Personal Information?
>
> We recognize the importance of maintaining the security of our customers' personal information. ***We use reasonable security measures, including physical, administrative, and technical safeguards to protect your personal information.***
>
> We have a team of associates who are responsible for helping to protect the security of your information. ***Whether you are shopping on our websites, through our mobile services, or in our stores, we use reasonable security measures, including physical, administrative, and technical safeguards.*** These measures may include physical and technical security access controls or other safeguards, information security technologies and policies, procedures to help ensure the appropriate disposal of information, and training programs.

(*Id*., ¶ 100.) However, in violation of this promise, and in violation of Defendant's statutory and common-law duties to safeguard the data, Defendant utilized a sloppy and incomplete security system, as is illustrated by the many vulnerabilities its systems pose. (*Id*., ¶ 101.)

III. ARGUMENT

A. Standard of Review.

Determining whether a plaintiff has failed to state a claim under Rule 12(b)(6) is a ruling on a question of law. *Parks School of Business, Inc., v. Symington*, 51 F.3d 1480, 1483 (9th Cir. 1995). "The issue is not whether the plaintiff ultimately will prevail, but whether he is entitled to offer evidence to support his claim." *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). Federal Rule of Civil Procedure 8(a)(2) requires only "a short and plain statement of the claim showing that the pleader is entitled to relief." "Specific facts are not necessary; the statement need only give the defendant fair notice of what the.... claim is and the grounds upon which it rests." *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (citations and internal quotations omitted). Although in order to state a claim a complaint "does not need detailed factual allegations, ... a plaintiff's obligation to provide the 'grounds of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.... Factual allegations must be enough to raise a right to relief above the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

speculative level." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 553-56 (2007) (citations omitted). A motion to dismiss should be granted if the complaint does not proffer "enough facts to state a claim for relief that is plausible on its face." *Id*. at 570. Review is limited to the contents of the complaint, *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754-55 (9th Cir. 1994), including documents physically attached to the complaint or documents the complaint necessarily relies on and whose authenticity is not contested. *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001). Allegations of fact in the complaint must be taken as true and construed in the light most favorable to the non-moving party. *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). The court need not, however, "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Id*.

B. Plaintiff States a Valid Claim Under the CCPA Because Plaintiff Adequately Pled Facts Showing that a Breach Occurred, and Plaintiff Pled that "Personal Information" Was Stolen.

1. By Pleading that the Data Is Presently for Sale on the Dark Web, Plaintiff Adequately Pled the Timing of the Exposure.

Under Cal. Civ. Code § 1798.150(a)(1), any consumer whose nonencrypted or nonredacted personal information "is subject to an unauthorized ***access and exfiltration, theft, or disclosure*** as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices" may institute a civil action for damages. (emphasis added). Plaintiff alleged that his and other consumers' personal information is currently available for sale on the dark web due to Defendant's violation of that duty. Plaintiff alleges "Plaintiff's Walmart account, and all of the data it contains, is currently being sold on the dark web." (Complaint, ¶ 7.) Plaintiff further alleges that "[o]ver two million accounts are available for sale at websites such as http://wwhclubl4tefzrzf.onion/index.php?threads/skupaju-gifty-amazon-carters-walmart-old-navy-pod-vysokij.58790/page-12, and http://blackpasqk3nqfuc.onion/shopps. Many similar websites exist. Plaintiff successfully identified many specific persons by name and address information provided by these websites, including himself." (*Id*., ¶ 15.) That is sufficient to show that, within the statutory period set forth in the CCPA, Plaintiff has alleged that he and the class

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

members' personal information was "subject to . . . disclosure." Cal. Civ. Code § 1798.150(a)(1).

Defendant argues, nonetheless, that Plaintiff's claim must fail because he does not allege the specific date when the data was compromised. Of course, while Plaintiff can identify the specific purchase which led to the disclosure, he cannot say when specifically Defendant's system was breached. But he need not do so to survive a motion to dismiss. Courts have consistently held that Plaintiffs need not plead specific dates when they have provided sufficient information for Defendants to identify and defend against the claim. "'[H]eightened fact pleading of specifics' is not required to survive a motion to dismiss." *Coupons, Inc. v. Stottlemire*, 588 F. Supp. 2d 1069, 1073 (N.D. Cal. 2008) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 127 S.Ct. 1955, 1973-74, 167 L.Ed.2d 929 (2007)). "Rather, the complaint need only 'give the defendant fair notice of what the ... claim is and the grounds upon which it rests.'" *Id*. (quoting *Erickson v. Pardus*, 551 U.S. 89, 127 S.Ct. 2197, 2200, 167 L.Ed.2d 1081 (2007)). By pleading that the personal information is currently posted on the dark web for sale, Plaintiff adequately put the defendant on fair notice that Plaintiff satisfied the time requirements of the CCPA because the disclosure is ongoing. Nothing more needed to be pled. *See Renfrow v. BDP Innovative Chemicals Co.,* No. CV-14-01183-PHX-GMS, 2015 WL 13036933, at *1 (D. Ariz. May 20, 2015) (rejecting the argument that a counterclaim was not sufficiently pled "because it does not include specific dates regarding the breach and, thus, does not allow Plaintiff to assess whether the relevant statute of limitations applies"); *Franco v. Grover*, No. CV-04-213-AHS SGL, 2005 WL 5955954, at *1 (C.D. Cal. Apr. 5, 2005) (rejecting defendant's argument that complaint was defective because it did not include specific dates when the alleged acts occurred).[1]

[1] *See also Taylor v. AFS Techs., Inc.*, No. CV-09-2567-PHX-DGC, 2010 WL 2228530, at *2 (D. Ariz. June 1, 2010) (despite the plaintiff's failure to include the specific date or dates when the plaintiff visited the subject premises, complaint survived because plaintiff provided "some notice as to when the challenged conduct allegedly occurred"); *Johnson v. Rehman*, No. 2:14-CV-01454-GEB-AC, 2014 WL 4986688, at *1–2 (E.D. Cal. Oct. 6, 2014) (same); *Matrix, Inc. v. Love Tree Fashion, Inc.*, No. 2:13-CV-04565-ODW, 2013 WL 4763869, at *1 (C.D. Cal. Sept. 4, 2013) (denying motion to dismiss "for not including the copyright registration number and specific dates for the allegedly infringing actions referenced in the Complaint"); *Priestley v. Newlin*, No. 14-CV-148-JL, 2016 WL 3023826, at *4 (D.N.H. Apr. 28, 2016), *report and recommendation approved sub nom. Priestley v. Tracy Newlin*, No. 14-CV-148-JL, 2016 WL 3024059 (D.N.H. May 24, 2016) ("In sum, the pleadings here are more than adequate to make Newlin aware of the claims he must defend against, even without pegging the claimed assault to a specific date."); *Major Tours, Inc. v. Colorel*, 720 F. Supp. 2d 587, 605 (D.N.J. 2010)

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Moreover, the reason that Plaintiff cannot state the specific date that the data was stolen is that Defendant has failed whatsoever to alert Plaintiff and the Class Members that a data breach occurred, which itself amounts to an ongoing violation of California law. Defendant cannot profit by its decision to hide the data breach by escaping liability for a cause of action that is in fact ongoing, as Defendant has done nothing to remove its customers' data from the dark web. This is true especially in light of the CCPA's stricture that the statute should be "liberally construed to effectuate its purposes." Cal. Civ. Code § 1798.194. Defendant cannot impose negative externalities on Plaintiff and the Class Members, resulting in ongoing data breaches, and escape liability under the CCPA by failing to provide notice. By pleading that the disclosure was ongoing, Plaintiff adequately pled that his claim fit within the timeframe of the CCPA.

2. Plaintiff Adequately Pled Loss of "Personal Information" Under the Applicable Definition.

The CCPA, in Cal Civ. Code § 1798.150(a)(1), incorporates the definition of "personal information" set forth in § 1798.81.5(A)(1)(d), which includes "An individual's first name or first initial and the individual's last name, in combination with . . . [a]ccount number or 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." With regard to a credit card or debit card, the access code or password which allows access to the card or the account is the expiration date in combination with the three-digit passcode on the back of the card. And it can be presumed that, when selling credit card numbers, black market vendors on the dark web are including this data. Otherwise, the numbers would be useless to criminals, and not worth the cost demanded for them. Under Rule 8(e) of the Federal Rules of Civil Procedure, "[p]leadings must be construed so as to do justice." *See also* 1 Gensler, Federal Rules of Civil Procedure, Rules and Commentary, Rule 8, at 164 (2020) (Rule 8(e) "stands as a reminder that, when enforcing the pleading requirements, courts must not exalt form over substance or rely on errors in draftsmanship to bar justice.")

(construing the complaint "so as to do justice," per Rule 8(e) of the Federal Rules of Civil Procedure, complaint adequately placed defendant on notice of claims despite the lack of a specific date); *Townsend v. Holt*, No. 3:13-CV-758, 2013 WL 4459023, at *5 (M.D. Pa. Aug. 16, 2013) (denying motion to dismiss for failure to provide specific dates when the acts occurred).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

(footnote and internal quotation marks omitted). Here, in pleading that the credit card information was available for sale on the dark web, it must be presumed that, among that information, was the expiration date of the cards in combination with the three-digit passcode on the back of the card, which is the information which allows access to the card and to the account. Notably, the Complaint states that "Plaintiff's Walmart account, and all of the data it contains, is currently being sold on the dark web." (Complaint, ¶ 7.) When Plaintiff entered his credit card information as a required step in the creation of his Walmart account, he also entered his card's expiration date and the security number on the back of the card. Otherwise, Walmart would not have been able to charge the card. Accordingly, the Complaint must be read as to allege that this security information, in addition to the card number, is available for sale on the dak web. *Spectrum Pac. W. LLC v. City of Yuma*, No. CV-20-01204-PHX-DWL, 2020 WL 7352634, at *4 (D. Ariz. Dec. 15, 2020) (omission that "amounted to no more than inartful pleading" did not justify dismissal) (quoting *Nationwide Mut. Ins. Co. v. Liberatore*, 408 F.3d 1158, 1162 (9th Cir. 2005)); *Nw. Corp. v. Econ. Research Grp., Inc.*, No. CV-08-04-BLG-RFC, 2008 WL 2532206, at *6 (D. Mont. June 24, 2008) (Complaint must be "'construed so as to do justice' under Rule 8(e), and . . . all reasonable inferences [must be] drawn in [plaintiff's] favor from the factual allegations supporting the claims.").

C. Plaintiff States At Least Four Valid Injury Theories Supporting His Claims.

Although some speculative harm is insufficient to constitute actual loss for purposes of a negligence claim, *Aas v. Super. Ct.*, 24 Cal.4th 627, 646, 101 Cal.Rptr.2d 718, 12 P.3d 1125 (2000), Plaintiffs put forward four injury theories which courts have held, in the data breach setting, constitute appreciable, non-speculative, and present harm for each of his claims.

1. Plaintiff's Loss of the Value of the PII Constitutes a Valid Injury Supporting Each Claim.

First, courts have held that a plaintiff's loss of value of her PII is sufficient harm. For instance, in *Anthem II*, 2016 WL 3029783, at *15, the court rejected defendant's argument that in order to successfully plead these damages plaintiff was required to plead "that there was a market for their PII *and* that they somehow also intended to sell their own PII," finding that

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

instead the plaintiff was required to plead only one of those two allegations. (emphasis in original.) Here, Plaintiff has alleged that there was a market for the PII. The Fourth Amended Complaint states that there is an "imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized third-party hackers and misused via the sale of Plaintiff's and Class Members' information on the Internet black market," and that there are "[a]scertainable losses in the form of deprivation of the value of [Plaintiff's] PII, for which there is a well-established national and international market." (Complaint at ¶ 42). Indeed, as the PII is currently being sold on a market, it cannot be denied that there is a market for the PII. As in *Anthem II*, "[t]hese allegations could be read to infer that an economic market existed for Plaintiffs' PII, and that the value of Plaintiffs' PII decreased as a result of the Anthem data breach." *Anthem II,* 2016 WL 3029783 at *15. "Presumably, the purpose of [a] hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id*. (quoting *Remijas v. Neiman Marcus Gp., LLC,* 794 F.3d 688, 693 (7th Cir. 2015). "Why else would hackers break into a store's database and steal consumer's private information?" *Id*. (quoting *Remijas,* 794 F.3d at 693; *see also In re Yahoo!,* 2017 WL 3727318, at *13 (holding that Plaintiffs had alleged an injury in fact where they alleged that the data breaches caused all plaintiffs to suffer a loss of value of their PII); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018), *cert. denied sub nom. Zappos.com, Inc. v. Stevens*, 139 S. Ct. 1373, 203 L. Ed. 2d 609 (2019) ("Although there is no allegation in this case that the stolen information included social security numbers, as there was in Krottner, the information taken in the data breach still gave hackers the means to commit fraud or identity theft . . .").

In *In re Facebook Privacy Litig.*, 572 Fed. Appx. 494, the Ninth Circuit expressly held that loss of value of PII could be sufficient to establish damages in a breach of contract claim, stating that "Plaintiffs allege that the information disclosed by Facebook can be used to obtain personal information about plaintiffs, and that they were harmed both by the dissemination of their personal information and by losing the sales value of that information," and that "[i]n the absence of any applicable contravening state law, these allegations are sufficient to show the element of damages for their breach of contract and fraud claims." *See also Svenson,* 2015 WL

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1503429 at *5 ("Svenson's allegations of diminution of value of her personal information are sufficient to show contract damages for pleading purposes."). The Ninth Circuit in *In re Facebook Privacy Litig.* did not require that the plaintiffs allege that they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from making such a sale, and subsequent courts have declined to apply those pleading requirements. *Id*. ("The Ninth Circuit holding does not require the type of explication" discussed by prior district court decisions); *see also Hameed Bolden v. Forever 21 Retail, Inc.*, No. CV1803019SJOJPRX, 2018 WL 6802818, at *5-6 (C.D. Cal. Oct. 1, 2018) ("In recent data breach cases, however, courts have found that the allegations that one's PII is a "valuable commodity" and that theft of this information results in loss of its sales value are sufficient to plead damages for breach of contract claims.")

As in *In re Facebook*, *Svenson*, *Anthem II*, and other cases, Plaintiff here clearly alleges deprivation of the value of the PII "for which there is a well-established national and international market." Indeed, unlike the cases cited by Defendant, Plaintiff has identified an actual market on which his PII is being sold. These allegations satisfy the harm requirement for Plaintiff's claims.

2. Plaintiff's Out-of-Pocket Expenses and Time Lost Pursuing Credit Monitoring Constitute a Valid Injury Supporting Each of His Claims.

Second, credit monitoring costs constitute compensable harm for purposes of each claim. *See* Restatement (Second) of Torts § 919 (1979) ("One whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened."); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *4–5 (C.D. Cal. June 15, 2015) ("[T]he Court finds that Plaintiffs adequately allege a cognizable injury by way of costs relating to credit monitoring, identity theft protection, and penalties."). Courts determining whether these injuries have been adequately stated typically look to a series of factors applied by the California courts to determine whether an injury supporting medical monitoring damages is present. (*Id*.) Those factors are:

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> (1) the significance and extent of the compromise to Plaintiffs' PII; (2) the sensitivity of the compromised information; (3) the relative increase in the risk of identity theft when compared to (a) Plaintiffs' chances of identity theft had the data breach not occurred, and (b) the chances of the public at large being subject to identity theft; (4) the seriousness of the consequences resulting from identity theft; and (5) the objective value of early detection.

Id. (citing *Potter v. Firestone Tire & Rubber Co.* (1993) 6 Cal.4th 965, 1008, 25 Cal.Rptr.2d 550, 863 P.2d 795). Applying them to a data breach case similar to this one, the court in *Corona* found that the factors supported a finding of compensable harm, reasoning, as to the first and second factors, that the public disclosure was of highly sensitive information, as to the third factor, that it was reasonable to expect that disclosure of the PII would drastically increase Plaintiff's risk of identity theft, as the fourth factor, that it was "commonly known that the consequences resulting from identity theft can be both serious and long-lasting," and that, as to the fifth factor, early detection was always of primary importance in a data breach, and in that case, reports of identity theft had already been received. *Id*.

As applied here, the *Corona* factors all weigh in favor of a finding of compensable harm. First, in this case Plaintiff's highly sensitive personal information, including name, address, and credit card information, including all information necessary to use the credit card, was implicated. This is highly sensitive information that was exposed to nefarious individuals. As to the third factor, as in *Corona*, it is reasonable to expect that theft of this personal information will drastically increase Plaintiff's risk of identity theft as compared to Plaintiff's odds had the breach not occurred and to the general public's risk of theft. Contrary to Defendant's assertions, it is not par for the course for one's credit card information to be sold on the dark web. And this information has not merely been exposed publicly; it is undoubtedly in the hands of criminals who are seeking to sell it to additional criminals. As in *Corona*, and as the Complaint alleges at great length, the consequences of identity theft can be both severe and long-lasting. And as in *Corona*, while here Plaintiff is not aware of any identity theft incurred by class members, it is likely that some identity theft has occurred, since over two million customers have had their data sold on the dark web, and early detection of the data breach is, as always, of primary importance. *C.f. Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323, 246 P.3d 877, 886 (2011) (economic injury includes being "required to enter into a transaction, costing

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

money or property, that would otherwise have been unnecessary"); *Witriol v. LexisNexis Grp.*, No. C05-02392 MJJ, 2006 WL 4725713, at *6 (N.D. Cal. Feb. 10, 2006) ("Plaintiff has expressly alleged that, he and the Class Members have incurred "costs associated with monitoring and repairing credit impaired by the unauthorized release of private information. Thus, Plaintiff has sufficiently alleged that he has suffered actual injury and sustained monetary loss as a result of Defendants' actions."); *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111-TSH, 2019 WL 7946103, at *9 (D. Mass. Dec. 31, 2019) *report and recommendation adopted*, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020) ("Because the risk that Plaintiffs' PII will be misused in the future is not so attenuated as to preclude a finding of an injury in fact, Plaintiffs' position concerning mitigation expenses bolsters their claim of imminent injury."); *In re Anthem*, 2016 WL 3029783 at *16 (defendants had "cited no binding precedent to suggest that Plaintiffs are precluded from recovering for specific types of Consequential Out of Pocket Expenses, such as credit monitoring, under California contract law."); *In re Yahoo! Inc. Customer Data Security Breach Litigation*, *supra*, 2017 WL 3727318 at p. *16 ("The Court finds that these allegations of out-of-pocket mitigation expenses are also sufficient to allege injury in fact arising from the Data Breaches.").

It is important to note that Plaintiff has alleged that he has already incurred credit monitoring costs. (*See* Complaint, ¶ 7.) However, under California law, future costs for the class members will also be obtainable. In *Corona v. Sony Pictures*, 2015 WL 3916744, at *4, the court analogized to California toxic tort cases which allow plaintiffs to recover damages for future medical costs associated with monitoring for a disease for which the plaintiffs have been put at risk. The seminal California case allowing for such damages is *Potter v. Firestone Tire & Rubber Co.*, 6 Cal.4th 965, 25 Cal.Rptr.2d 550, 863 P.2d 795 (1993). The *Potter* court did not limit the damages at issue to costs that had already been incurred, instead emphasizing that the plaintiff could obtain damages for future expenses. *Id*. at 1004-05 ("In the context of a toxic exposure action, a claim for medical monitoring seeks to recover the cost of *future* periodic medical examinations intended to facilitate early detection and treatment of disease caused by a plaintiff's exposure to toxic substances.") (emphasis added). Indeed, California courts have

consistently awarded damages for monitoring that has not yet taken place. *See, e.g., Garcia v. Duro Dyne Corp.*, 156 Cal.App.4th 92, 98 (2007) ("The fact that the amount of future damages may be difficult to measure or subject to various possible contingencies does not bar recovery."). As the court in *Miranda* recognized, requiring actual physical injury to recover in tort would not be consistent with California Civil Code section 3333, which states: "For the breach of an obligation not arising from contract, the measure of damages, except where otherwise expressly provided by this Code, is the amount which will compensate for all the detriment proximately caused thereby, whether it could have been anticipated or not." *Miranda v. Shell Oil Co.* 17 Cal.App.4th 1651, 1655-57 (1993).

For purposes of this motion, however, Plaintiff has clearly alleged that he has paid for credit monitoring. (Complaint, ¶ 7) ("Consequently, as a necessary and reasonable measure to protect himself, Plaintiff purchased a credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat risk of further identity theft."). And the necessity for this credit monitoring is clear: Plaintiff's personal information was, as of the time of the filing of the Complaint, available for sale on the dark web. This is not a remote threat of harm, but a substantially likely threat that the data will be obtained and misused.

3. Plaintiff States an Adequate Injury for his Contract-based and UCL Claims Under the Benefit of the Bargain Theory.

Under Cal. Civ. Code § 3300, "[f]or the breach of an obligation arising from contract, the measure of damages, except where otherwise expressly provided by this Code, is the amount which will compensate the party aggrieved for all the detriment proximately caused thereby, or which, in the ordinary course of things, would be likely to result therefrom."[2] These damages have been termed the "benefit of the bargain." *See KGM Harvesting Co. v. Fresh Network*, 36 Cal.App.4th 376, 382 (1995) ("The basic premise of contract law is to effectuate the expectations of the parties to the agreement, to give them the 'benefit of the bargain' they struck

[2] *See also Oakland California Towel Co. v. Sivils*, 52 Cal.App.2d 517, 519 (1942) ("Ordinarily in an action such as the present, the measure of damages is the amount which will compensate the party aggrieved for the detriment proximately caused by the breach.").

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

when they entered into the agreement.").[3] Here, Plaintiff asserts that he paid for goods and accepted prices that he would not have accepted had he known that his PII would not be protected. The differences in prices between what he paid and/or accepted and what he would have paid and/or accepted are the direct benefit of the bargain damages which Plaintiff is owed.

In *Anthem II*, 2016 WL 3029783 at *13-14, the court found that the plaintiffs had adequately pled damages for their breach of contract claim by alleging that they had paid more for insurance premiums than they would have paid had they known that their data would not be protected. The court specifically rejected the defendant's argument that the plaintiffs' benefit of the bargain theory failed because plaintiffs did not "allege facts showing that any alleged payments were earmarked for data security," finding that "the Anthem Defendants have identified no California or Ninth Circuit authority to suggest that an entity must precisely 'earmark' what portion of Plaintiffs' premiums want towards protecting Plaintiffs' data privacy." *Id*. at *13. "Put another way, the Anthem Defendants can not evade liability because the Anthem Defendants did not provide, in advance, a breakdown on how much of Plaintiffs' premiums the Anthem Defendants allocated (or should have allocated) to protecting Plaintiffs' PII." *Id*. at *14; *see also Svenson v Google Inc.*, 2015 WL 1503429 at *4 (N.D. Cal. 2015) (holding, in a data breach case, that plaintiff had "alleged facts sufficient to show contract damages under a benefit of the bargain theory.").

Similarly, in *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197, 1223-24 (N.D. Cal. 2014), the court found that the plaintiff in a data breach case had properly alleged economic injury on a benefit of the bargain theory, observing that "[p]laintiffs allege they personally spent more on [defendant's] products than they would had they known [defendant] was not providing the reasonable security [defendant] represented it was providing," finding that it was "plausible that a company's reasonable security practices reduce the risk of theft of customer's personal data and thus that a company's security practices have economic value,"

[3] "The basic object of damages is *compensation*, and in the law of contracts the theory is that the party injured by the breach should receive as nearly as possible the equivalent of the benefit of performance." *Ibid*. (quoting *Lisec. v. United Airlines, Inc.*, 10 Cal.App.4th 1500, 1503, 11 Cal.Rptr.2d 689 (1992)).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

and on that basis finding that plaintiffs had "plausibly pleaded" that "they [had] personally lost money or property as a result" of defendant's failures."[4] Plaintiff has clearly alleged that he conferred a benefit on Defendant in exchange for services which he did not receive. He has pled benefit of the bargain damages.

4. Plaintiff Adequately Alleges Injury for Each of His Claims by Alleging Future Risk of Identity Theft.

Courts have widely found that an increased risk of future identity theft resulting from a data breach constitutes a compensable injury. *See In re Yahoo!,* 2017 WL 3727318 at *13 (Plaintiffs who alleged that their private information stored in Yahoo! accounts was accessed by hackers "have alleged a 'credible threat of real and immediate harm' stemming from the data breaches.") (quoting *Krottner v. Starbucks Corp.* 628 F.3d 1139, 1143 (9th Cir. 2010) ("Plaintiffs–Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."); *In re Zappos.com, Inc.*, 888 F.3d at 1028 (plaintiffs who suffered compromise of data, like Plaintiff here, were placed at "imminent risk of identity theft"); *Bass v. Facebook,* 2019 WL 2568799 at *7 (N.D. Cal. 2019) (holding that "between the obvious goal of taking personal information, the nature and amount of information taken," and other evidence of data breach, "plaintiff Adkins has plausibly shown he is at risk of further fraud and identity theft."); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x. 384, 388 (6th Cir. 2016) ("Where data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.").

Plaintiff alleges that hackers stole their PII from Defendant. Under precedent, it can be presumed that the hackers did so in order to misuse that information. *Id*. But here, it does not even need to be presumed, because the hackers are in fact selling the data to criminals on the

[4] (*See also Hameed-Bolden v. Forever 21 Retail, Inc.* 2018 WL 6802818 at *3 (C.D. Cal. 2018) (holding that contract damages were adequately pled where "[p]laintiffs argue that by failing to secure the Customer Data, [d]efendants did not provide full compensation for the benefit the [p]laintiffs and [c]lass members provided."); *In re Yahoo!,* 2017 WL 3727318 at *16-17 ("The Court finds that Neff's allegations are sufficient to allege 'benefit of the bargain' losses as a result of the Data Breaches, which courts in this district and elsewhere have found are sufficient to allege an injury in fact for purposes of Article III standing.").

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

dark web. Plaintiff alleges that he has thus been "placed at an imminent, immediate, and continuing risk of identity theft-related harm." (Complaint ¶ 73). That is sufficient to plead damages under the overwhelming weight of authority.

Defendant alleges that Plaintiff cannot show increased risk of identity theft due to allegations that, among he and the class members, some credit card accounts were modified or cancelled as a result of the breach. To the extent that these allegations appear to state that Plaintiff's own credit cards were cancelled, they are the product of an error in drafting. Plaintiff did not cancel his credit cards, and does not even know for sure which credit cards were compromised, as he does not know which were used. Plaintiff has not purchased his own data on the dark web. The allegations were meant to include class members who had cancelled their credit cards. Amendment may be granted liberally to cure drafting errors in pleadings. *Okeke v. Biomat USA, Inc.*, 927 F. Supp. 2d 1021, 1029–30 (D. Nev. 2013) ("Given the obvious nature of this drafting error and the liberal policy permitting amendment under the Federal Rules, leave to amend with respect to this particular error (and a similar error in paragraph 3) is granted."); *Diversified Capital Investments, Inc. v. Sprint Commc'ns, Inc.*, No. 15-CV-03796-HSG, 2016 WL 2988864, at *10 (N.D. Cal. May 24, 2016) ("Plaintiff may amend its complaint to correct the drafting error discussed above and its proposed class definition as it has requested."). Accordingly, to the extent that the Court's ruling turns on this point, Plaintiff respectfully requests leave to amend.

D. Plaintiff Adequately States a UCL Claim.

1. Plaintiff Has UCL Standing.

Defendant also attempts to challenge Plaintiff's UCL standing while ignoring a wealth of cases holding that Plaintiff's specific damages theories supply that standing. Benefit of the bargain damages have been found sufficient to confer UCL standing in many data breach cases. *See Svenson v. Google Inc.*, No. 13-CV-04080-BLF, 2015 WL 1503429, at *8 (N.D. Cal. Apr. 1, 2015) ("Svenson thus alleges that she paid Google for services that she did not receive as a result of Google's unlawful and unfair business practices, establishing economic injury."); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

*21 (N.D. Cal. Aug. 30, 2017) (allegations that the plaintiff would not have agreed to pay for the small business services and turn over his PII had he known that the PII would not be adequately secured "adequately alleged standing under the UCL"); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985–87(N.D. Cal. 2016) ("*Anthem I*") ("more recent case law within the data breach context confirms that benefit of the bargain damages represent economic injury for purposes of the UCL.") (citing *In re Adobe Sys., Inc. Privacy Litig.*, 66 F.Supp.3d 1197, 1224 (N.D. Cal. 2014) (finding standing under the UCL because "[f]our of the six [p]laintiffs allege they personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing."); *In re LinkedIn User Privacy Litig.*, 2014 WL 1323713, *4 (N.D. Cal. Mar. 28, 2014) (finding that benefit of the bargain losses are "sufficient to confer...statutory standing under the UCL."); *In re Marriott Interntional, Inc., Customer Data Security Breach Litigation*, No. 19-MD-2879, 2020 WL 869241, at *35 (D. Md., Feb. 21, 2020) (holding that UCL standing existed because "[h]ere, like the plaintiffs in *Anthem*, *Adobe*, and *LinkedIn*, Plaintiffs have sufficiently alleged benefit-of-the-bargain losses.").

In losing control of his PII, Plaintiff also suffered a diminishment of a present or future property interest. *See Kwikset*, 51 Cal.4th at 324. Numerous courts have held that loss of value of PII resulting from exposure of that PII to hackers is a sufficient injury to confer Article III standing. *See, e.g., In re Yahoo! Inc. Customer Data Security Breach Litigation*, 2017 WL 3727318, at *14 ("Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from the Data Breaches."); *In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783, at *15 (Plaintiff adequately alleged injury of loss of value of PII by alleging either that there was an economic market for the PII or that it would be harder to sell the PII, not both). So too, these injuries should be considered losses of money or property for purposes of UCL standing. The Complaint illustrates just why that is so. PII is coveted by hackers, stolen by them, and sold on the dark web, because it is an item of value. If it were not valuable, nefarious

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

actors would not take efforts to obtain it. But not only nefarious actors recognize this value. Companies like Facebook openly traffic in user data. It is a commodity. By losing control of his PII, Plaintiff lost its value, which constitutes a loss of money or property under the UCL.

Further, Plaintiff has alleged that he has paid and will have to pay additional money for credit monitoring services that he would not have required had Defendant protected the PII, as promised. These are direct monetary losses which confer standing under the UCL. *See, e.g., Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *5 (C.D. Cal. June 15, 2015) ("[T]he Court finds that [p]laintiffs adequately allege a cognizable injury by way of costs relating to credit monitoring, identity theft protection, and penalties."); *Witriol v. LexisNexis Grp.*, 2006 WL 4725713, *6 (N.D. Cal. Feb. 10, 2006) ("Plaintiff has expressly alleged that[ ] he and the Class Members have incurred costs associated with monitoring and repairing credit impaired by the unauthorized release of private information. Thus, plaintiff has sufficiently alleged that he has suffered actual injury and sustained monetary loss as a result of [d]efendants' actions.") (internal quotation marks omitted); *Hameed-Bolden v. Forever 21 Retail, Inc.*, No. CV1803019SJOJPRX, 2018 WL 6802818, at *4 (C.D. Cal. Oct. 1, 2018) (Plaintiffs' allegations that they "lost money and time" as a result of the data breach constitutes economic damage for purposes of UCL standing); *Walters v. Kimpton Hotel & Restaurant Group, LLC*, No. 16-CV-05387-VC, 2017 WL 1398660, at *2 (N.D. Cal., Apr. 13, 2017) (holding that plaintiff suffered an economic injury conferring UCL standing where he alleged that he spent time and effort monitoring credit).

2. There Is No Adequate Remedy at Law.

"A plaintiff seeking equitable relief in California must establish that there is no adequate remedy at law available." *Philips v. Ford Motor Co.*, No. 14–CV–02989–LHK, 2015 WL 4111448, at *16 (N.D. Cal. July 7, 2015) (citing *Knox v. Phoenix Leasing, Inc.*, 29 Cal. App. 4th 1357, 1368 (1994)); *see also Schroeder v. United States*, 569 F.3d 956, 963 (9th Cir. 2009) ("[E]quitable relief is not appropriate where an adequate remedy exists at law."). Here, there is no adequate remedy at law, supporting both injunctive relief and restitution. Defendant argues Plaintiff has failed to show that there is no adequate remedy at law while, in the next breath,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

arguing that Plaintiff's alternative theories for remedies at law are all deficient. If Defendant is correct that Plaintiff cannot state a claim under his other causes of action, it cannot be denied that he has no adequate remedy at law, and that his UCL claim must therefore go forward.

But even if Plaintiff's remedies at law are available, they are still inadequate. First, as to injunctive relief, Plaintiff seeks to prevent Defendant from continuing to leave its customers vulnerable to identity theft. No award of monetary damages will force Defendant to protect its customers by adopting industry-standard, reasonable safeguards. Nothing will stop innumerable innocent and guileless consumers from paying for products and providing their PII to Defendant under the false impression that Defendant is protecting that PII. An injunction is, by its nature, forward-looking. "The purpose of a prohibitory injunction is to prevent future harm to the applicant by ordering the defendant to refrain from doing a particular act." *Huntingdon Life Scis., Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.*, 129 Cal. App. 4th 1228, 1266, 29 Cal. Rptr. 3d 521, 551 (2005) (citation omitted). There is no adequate remedy at law which will prevent Defendant from continuing to leave its customers open to fraudulent use of their credit cards while representing to those customers that it is doing its very best to stop that from happening; accordingly, there is no adequate remedy at law which will grant Plaintiff the relief that his injunction seeks.

Second, as to restitution, Plaintiff seeks a full refund of the price he paid for products he purchased from Walmart. Under his actions at law, Plaintiff will not receive the full price he paid for those products. Restitution has two purposes: "to restore the defrauded party to the position he would have had absent the fraud," and "to deny the fraudulent party any benefits, whether or not for[e]seeable, which derive from his wrongful act." *Nelson v. Serwold*, 687 F.2d 278, 281 (9th Cir.1982) (citing the Restatement of Restitution). Those purposes are only served by a return of Plaintiff's full purchase price. However, as noted, that remedy is not available at law. Therefore, Plaintiff has no adequate remedy at law.[5]

[5] Defendant also takes issue with Plaintiff's unlawful prong allegations. First, the allegations as to the violation of the FTC Act are made in sufficient detail to withstand a motion to dismiss. *Estate of Fuller v. Maxfield & Oberton Holdings, LLC*, 906 F. Supp. 2d 997, 1012 (N.D. Cal. 2012) ("Plaintiff has alleged facts sufficient to withstand a motion to dismiss on the § 3344.1 and Lanham

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

E. The Economic Loss Doctrine Does Not Apply to Plaintiff's Negligence Claim.

Walmart seeks to hide behind the economic loss doctrine. However, the California Courts of Appeal have never applied the economic loss doctrine to negligence cases arising from data breaches, and there is good reason to suspect that the economic loss doctrine cannot apply in that context. Under the "economic loss" rule, "in actions for negligence, a manufacturer's liability is limited to damages for physical injuries; no recovery is allowed for economic loss alone." *Aas*, 24 Cal. 4th at p. 636. Here, there is no manufacturer or builder; the doctrine simply does not apply. In *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 127 (D. Me. 2009), *aff'd in part, rev'd in part sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011), the court specifically rejected the application of the economic loss doctrine to data breach cases.[6] Moreover, the purpose of the economic loss rule, to protect the distinction between warranty and strict products liability, issues not found here, counsels against its application. *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004); *see also N. Am. Chem. Co. v. Sup. Ct.*, 59 Cal. App. 4th 764, 781-788 (1997) (economic loss rule does not apply in cases involving negligent performance of services that result in foreseeable economic loss).

1. Plaintiff's Negligence Claim is Based on Statutory and Regulatory Duties Which Are Independent of the Contracts.

The economic loss doctrine plainly does not apply when the defendant has breached a duty which is independent of the contract at issue. *Aas*, 24 Cal. 4th at p. 643 ("conduct amounting to a breach of contract becomes tortious when it also violates a duty independent of the contract arising from principles of tort law."); *see also Erlich v. Menezes*, 21 Cal. 4th 543, 551–52, 981 P.2d 978, 982–83 (1999) ("the same wrongful act may constitute both a breach of

---

Act claims, and has thus stated a claim under the "unlawful" prong.). Second, Defendant ignores the fact that Plaintiff has also stated a claim under the "unfair prong," which independently gives rise to liability.

[6] Indeed, while California courts have yet to squarely address the application of the economic loss doctrine to data breach cases, the Supreme Court of Florida recently held that the economic loss doctrine was strictly limited to products liability cases. *See Tiara Condo. Ass'n, Inc. v. Marsh & McLennan Companies, Inc.*, 110 So. 3d 399, 407 (Fla. 2013) ("the application of the economic loss rule is limited to products liability cases").

contract and an invasion of an interest protected by the law of torts.") (quoting *N. Am. Chem. Co. v. Super. Ct.*, 59 Cal.App.4th 764, 774, 69 Cal.Rptr.2d 466 (1997) (citing 3 Witkin, Cal. Procedure, Actions, § 139 pp. 203–204 (4th ed. 1996))); *Fuentes v. Perez*, 66 Cal. App. 3d 163, 167, 136 Cal. Rptr. 275, 276 (1977) ("It is of course settled that a breach of contract may also be tortious, and that the injured party in such a case may recover either in contract, or in tort."); *Acadia, California, Ltd. v. Herbert*, 54 Cal. 2d 328, 336–37 (1960) (jury correctly awarded punitive damages on tort theory where parties' relationship was also governed by a contract because "[a]n act that constitutes a breach of contract may also be tortious"); *Robinson Helicopter*, 34 Cal.4th at p. 992 ("Simply put, a contract is not a license allowing one party to cheat or defraud the other.") (internal quotation omitted).

Such is the case here. Defendant has violated the CCPA, Cal. Civ. Code § 1798.150 *et seq.*, the Federal Trade Commission Act, 15 U.S.C. § 45, and Cal. Civ. Code § 1798.81.5, each of which creates a duty independent of Defendant's contracts with Plaintiff requiring Defendant to use adequate measures to protect the PII, the breach of which creates a cause of action for negligence. In each case, Defendant's conduct violates a duty independent of the contract. *Aas*, 24 Cal. 4th at p. 643. Accordingly, the economic loss doctrine does not apply.

2. Plaintiff Has Stated a Non-Economic Harm in the Form of Loss of Time Spent Monitoring His Credit.

Even if the Plaintiff had not articulated three independent duties which Defendant has violated, the economic loss doctrine would not preclude recovery because Plaintiff has identified a non-economic harm resulting from the data breach, namely, loss of time spent checking credit and taking preventative measures against identity theft. In *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019), the court held that the economic loss rule did not bar the plaintiff's negligence claim, in which he alleged that the defendant had breached its duty of care by failing to take adequate measures to prevent a data breach, because the plaintiff alleged "loss of time" as harm, holding, "plaintiff alleged his loss of time as harm and so does not allege pure economic loss. The economic loss rule therefore does not apply." As in *Bass*, Plaintiff here alleges loss of time as a non-economic loss. (Complaint, ¶ 42)

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

("Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach."). Therefore, the economic loss rule does not apply.

3. Plaintiff and Defendant Have a Special Relationship Which Overrides the Economic Loss Doctrine.

California courts also recognize an exception to the economic loss doctrine where a special relationship exists between the plaintiff and the defendant. *J'Aire Corp. v. Gregory* (1979) 24 Cal.3d 799. It is no longer a requirement that the parties lack contractual privity in order to apply the special relationship doctrine. *Stop Loss Ins. Brokers, Inc.,* 143 Cal. App. 4th at 1061 ("[s]ubsequent cases have extended the application of *J'Aire* to cases where the parties are in contractual privity. [Citation.] ... "[T]he reasoning of *J'Aire* is wholly incompatible with a limitation of the cause of action to those instances in which the plaintiff and defendant are not in privity.'") (quoting *North American Chemical Co.*, 59 Cal.App.4th at 783).

The necessary "special relationship" is established by consideration of the following six criteria: "(1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct, and (6) the policy of preventing future harm." *Id*. at p. 782. Of these factors, it is the second, "the foreseeability of the economic harm to the plaintiff from the defendant's negligent conduct" which is the "critical factor." *Id*. (citing *J'Aire*, 24 Cal.3d at 805-806.)

All the factors weigh in favor of finding a special relationship between Plaintiff and Defendant. First, the transaction, in which Plaintiff purchased goods from Walmart, was undoubtedly entered for the purpose of benefiting Plaintiff. As to the second, most critical factor, Plaintiff, whose sensitive PII was being handled pursuant to this transaction, was subject to foreseeable harm should that PII be exposed and accessed, as it was, to unauthorized users. All parties to the contracts could foresee that Plaintiff would suffer harm if his PII was exposed due to the significant risk of identity theft and other fraud. As to the third factor, as shown

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

above, there is high certainty that Plaintiff has suffered harm by (a) suffering an increased risk of identity theft, (b) losing the value of his PII, and (c) being forced to incur mitigation costs for identity theft protection. As to the fourth factor, there is a close connection between Defendant's conduct and the injury suffered in that, by failing to adequately protect the PII from exposure, Defendant enabled unauthorized users to obtain it. As to the fifth factor, significant moral blame should be attached to Defendant's conduct. Individuals cannot purchase goods online without relying on vendors like Walmart to protect the PII that they must provide to complete the transactions. Therefore, to participate fully in the economy, individuals must trust companies such as Defendants with their sensitive PII. It is blameworthy to abuse that trust by failing to protect the PII from hackers. It also hurts our nation's economy, which cannot succeed where partners to transactions cannot trust each other. As to the sixth factor, the policy of preventing future harm lies in favor of finding a special relationship here. If companies such as Defendants are to be adequately deterred from allowing PII to go unprotected, they must pay for the foreseeable harm that their conduct causes.

F. The Contract Claims Survive Because the Limitation of Liability and Disclaimer of Warranty Clauses Are Unconscionable.

"With respect to claims for breach of contract, limitation of liability clauses are enforceable unless they are unconscionable, that is, the improper result of unequal bargaining power or contrary to public policy." *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*, 209 Cal. App. 4th 1118, 1126 (2012). "Under California law, a contractual clause is unenforceable if it is both procedurally and substantively unconscionable." *Davis*, 485 F.3d at 1072 (citing *Armendariz v. Found. Health Psychcare Servs., Inc.*, 24 Cal.4th 83, 99 Cal.Rptr.2d 745, 6 P.3d 669, 690 (2000); *Nagrampa*, 469 F.3d at 1280. Courts apply a sliding scale: "the more substantively oppressive the contract term, the less evidence of procedural unconscionability is required to come to the conclusion that the term is unenforceable, and vice versa." *Armendariz*, 99 Cal.Rptr.2d 745, 6 P.3d at 690.

Under California law, contracts of adhesion are *per se* procedurally unconscionable. *Sanchez v. Valencia Holding Co., LLC*, 61 Cal. 4th 899, 913–15, 353 P.3d 741, 750–51 (2015)

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

("Here the adhesive nature of the contract is sufficient to establish some degree of procedural unconscionability."). Because the contract at issue is a form contract presented to a consumer on a take-it-or-leave-it basis, with no opportunity to negotiate its terms, it is a contract of adhesion, and is, therefore, procedurally unconscionable for that reason alone. *Id*; *see also Gutierrez v. Autowest, Inc.*, 114 Cal.App.4th 77, 89, 7 Cal.Rptr.3d 267, 276-277 (2003), *as modified on denial of reh'g* (Jan. 8, 2004) (The plaintiff "either had to accept the arbitration clause and the other preprinted terms, or reject the lease entirely. Under these circumstances, the arbitration clause was procedurally unconscionable."). Plaintiff was "not given 'reasonable notice of [the] opportunity to negotiate or reject the terms of a contract, and ... an actual, meaningful, and reasonable choice to exercise that discretion.'" *Parada v. Superior Court*, 176 Cal.App.4th 1554, 1570-71, 98 Cal.Rptr.3d 743 (2009) (quoting *Circuit City Stores, Inc. v. Mantor*, 335 F.3d 1101, 1106 (9th Cir. 2003)). The clause is, therefore, procedurally unconscionable.

But the limitation of liability and disclaimer of warranty clauses are procedurally unconscionable for another important reason. In the Privacy Policy, Walmart sets forth a clear promise that it will protect the PII from disclosure to unauthorized third parties, using "reasonable security measures, including physical, administrative, and technical safeguards to protect your personal information." (Complaint, ¶ 100). In the limitation of liability section, Walmart purports to make that promise wholly illusory, by declaiming liability for failing to take the very protective measures it promises to take. By making a promise and, in effect, taking it back in another section, Walmart creates confusion on the part of the consumer, who might not know which provision controls over the other. That confusion is, under California law, a source of procedural unconscionability. *See, e.g., Harper v. Ultimo*, 113 Cal.App.4th 1402, 1406, 7 Cal.Rptr.3d 418 (2003) (holding that it was oppressive to reference the Better Business Bureau rules but not attach them to the agreement because the customer must go to another source to determine the impact of what he is signing); *Brown v. MHN Gov't Servs., Inc.*, 178 Wash. 2d 258, 267–68, 306 P.3d 948, 954–55 (2013) (applying California law) ("However, the arbitration agreement contains procedural surprise due to its lack of clarity regarding which set of AAA rules would govern the arbitration.").

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Because procedural unconscionability is high, under the sliding scale, a lesser amount of substantive unconscionability will suffice. *Armendariz*, 99 Cal.Rptr.2d 745, 6 P.3d at 690. However, there is also an extremely high level of substantive unconscionability here. The clauses purport to waive liability for all damages of any kind resulting from Plaintiff's relationship with Defendant. These clauses render the Terms of Use a contract which cannot be enforced, in any manner, by Plaintiff, making the contract completely illusory. Yet, in providing contract terms, which include specific promises, Defendant creates the impression that there are terms which do in fact bind Defendant, and promises which can in fact be enforced. Defendant essentially seeks to bind Plaintiff to contract terms while remaining completely unaccountable to Plaintiff in any manner whatsoever. If these terms are enforced, and Defendant is not liable in any manner for any promise made, then there essentially is no contract, and Plaintiff should be permitted to proceed on a quasi-contract or implied contract theory. But under California law, clauses which create illusory contracts are themselves unconscionable. "The paramount consideration in assessing substantive conscionability is mutuality." *Nyulassy v. Lockheed Martin Corp.*, 120 Cal. App. 4th 1267, 1281, 16 Cal. Rptr. 3d 296, 306 (2004) (internal quotation omitted). For instance, unilateral agreements to arbitrate have been held to be unconscionable. *Id*; *see also Abramson v. Juniper Networks, Inc.*, 115 Cal. App. 4th 638, 665, 9 Cal. Rptr. 3d 422, 443–44 (2004) ("This carve-out in the employment contract thus addresses only the employee's breach of covenants designed to protect only the employer's interests. It therefore lacks mutuality, both facially and operationally."). It follows that a provision which renders an entire contract to be unilateral is also unconscionable.

As the provisions at issue are both substantively and procedurally unconscionable, they must be severed from the Terms of Use, and Plaintiff's contract-based claims be permitted to go forward.

IV. CONCLUSION

For the reasons expressed herein, respectfully, the Court should deny Defendant's motion in its entirety. Should the Court in its discretion choose to grant the motion in any respect, Plaintiff respectfully requests leave to amend.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Respectfully submitted,

Dated: January 13, 2021

WILSHIRE LAW FIRM, PLC

By: /s/ Robert J. Dart

Justin F. Marquez
Thiago M. Coelho
Robert J. Dart
Attorneys for Plaintiffs and the Proposed Class

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137