IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 17-cv-1415-CMA-MLC

TODD GORDON, *et al.*, individually and
on behalf of all others similarly situated,

Plaintiffs,

v.

CHIPOTLE MEXICAN GRILL, INC.,

Defendant.

RECOMMENDATION ON MOTION TO DISMISS

Magistrate Judge Mark L. Carman

This purported class action regards a data breach that Defendant Chipotle Mexican Grill, Inc. ("Chipotle") experienced in early 2017. Doc. 36 (Am. Complaint) ¶ 1. Plaintiffs Todd Gordon, Marc Mercer, Kristen Mercer, Kristin Baker, Michelle Fowler, Greg Lawson and Judy Conrad allege they used credit or debit cards to make purchases at Chipotle restaurants during the data breach.[1] They allege their personally identifiable information ("PII") was thereby compromised, and consequently they had to take steps to redress fraud and protect themselves from further fraud, including identity theft. On their own behalf and that of others similarly situated, Plaintiffs bring several tort, contract, statutory and equitable claims, apparently under the laws of the states in which they made the purchases. The court has subject matter jurisdiction

[1] Another action brought by financial institutions regarding the same breach is also pending. *Bellwether Cmty. Credit Union v. Chipotle Mexican Grill, Inc.*, Civ. 17-1102-WJM-STV.

under the Class Action Fairness Act of 2005 (28 U.S.C. § 1332(d)(2)(A)) and supplemental jurisdiction under 28 U.S.C. § 1367.

Defendant moves to dismiss the claims of Plaintiffs Kristin Baker and Greg Lawson for lack of standing. Defendant further moves to dismiss all claims for failure to state a claim. Judge Christine M. Arguello referred the motion to the undersigned magistrate judge for a recommendation. As follows, the court recommends granting in part and denying in part.

I. BACKGROUND

Plaintiffs allege Chipotle used inadequate measures to secure customers' payment card information it received at most of its stores in the continental United States. Among other things, Plaintiffs point in particular to Chipotle's alleged decision to not implement the payment card industry's ("PCI") "EMV technology," where EMV stands for "Europay, MasterCard and Visa." Doc. 36 ¶¶ 1–9. EMV technology is a "'global standard' for cards equipped with computer chips and technology used to authenticate chip card transactions" which generates a "unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen." *Id.* ¶ 68.

Plaintiffs allege that because Chipotle did not implement EMV technology (or other reasonable measures), its point of service ("POS") systems were vulnerable to malware that fraudsters had used several times to infiltrate other major retailers' POS, in order to steal payment card information. According to Chipotle's announcement, it discovered the malware had been operative on its POS systems from March 24, 2017 to April 18, 2017. Doc. 36 ¶ 1. Chipotle allegedly did not "timely and accurately notify Plaintiffs and Class Members that their personal and financial information had been compromised," *Id.* ¶ 2, and did not offer assistance, such as

free credit monitoring. Doc. 36 ¶¶ 8, 102-04. Plaintiffs assert Chipotle has still "not disclosed exactly what type of information was in fact exfiltrated in the Data Breach." *Id.* ¶ 32.

Plaintiffs allege their individual payment card purchases from Chipotle during the time of the data breach and specific harms each individual allegedly incurred due to the data breach. Doc. 36 ¶¶ 10–18. Overall, they allege Chipotle's data breach caused them

> loss of time and money resolving fraudulent charges [and] ... obtaining protections against future identity theft; financial losses related to the purchases ... that Plaintiffs and Class members would have never made had they known of Chipotle's careless approach to cybersecurity; lost control over the value of personal information; ... losses and fees relating to exceeding credit and debit card limits and balances, and bounced transactions; [and] harm resulting from damaged credit scores and information....

Id. ¶ 88.[2] Plaintiffs also allege Chipotle's misconduct has "placed [them] at [an] increased risk of harm from identity theft," to protect against which they are "placing 'freezes' and 'alerts' with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts." *Id.* ¶ 89. Plaintiffs seek several types of damages, penalties, equitable relief, injunctive relief, and declaratory relief, and their attorneys' fees and costs. *Id.* at 74 (prayer for relief).

II. ANALYSIS

A. Standing of Plaintiffs Baker and Lawson

Defendant argues Kristin Baker and Greg Lawson do not plausibly allege injuries that would satisfy the Article III "case" or "controversy" requirement for subject matter jurisdiction. Standing is first and foremost concerned with whether a plaintiff has suffered an "injury in fact," such that resolution of his or her claim involves the judicial power, not the executive or legislative. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 559-60 (1992). *See also Clapper v. Amnesty Int'l*

[2] This paragraph also alleges unreimbursed losses relating to fraudulent charges, but only one Plaintiff alleged such and the charges have since been reversed. Doc. 57 (Response) at 4, n.1.

USA, 568 U.S. 398, 408 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches."). Standing requires the plaintiff to show he or she has

> suffered an "injury in fact"—an invasion of a legally protected interest which is (a) concrete and particularized ... and (b) "actual or imminent, not 'conjectural' or 'hypothetical,' ... Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be "fairly ... trace[able] to the challenged action of the defendant, and not ... th[e] result [of] the independent action of some third party not before the court." ... Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."

Lujan, 504 U.S. at 560-61 (internal citations omitted).

Plaintiffs bear the burden of proving standing. *See, e.g., Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1547 (2016) (as revised May 24, 2016). When standing is raised at the Rule 12 stage, the showing required depends whether the defendant raises a facial or factual challenge. *Holt v. United States*, 46 F.3d 1000, 1002-3 (10th Cir. 1995). A "facial attack on the complaint' s allegations as to subject matter jurisdiction questions the sufficiency of the complaint," and in reviewing such an attack "a district court must accept the allegations in the complaint as true." *Pueblo of Jemez v. United States,* 790 F.3d 1143, 1148 n.4 (10th Cir. 2015) (citing *Holt*). In this case, Defendant brings a facial challenge, as it does not raise facts outside the complaint for this issue. Therefore, Plaintiffs must show their allegations plausibly support standing. *Lujan*, 504 U.S. at 561 (standing must be shown "with the manner and degree of evidence required at the successive stages of the litigation.").

Here, Defendant takes issue with the "injury in fact" element with respect to Lawson and Baker.[3] Defendant raises three arguments. First, Defendant argues Lawson and Baker assert a

[3] Defendant also mentions Lawson and Baker's harms are not traceable to its conduct but provides no argument in support. Even if the issue had been properly raised, Baker alleges misuse of her stolen payment card information within a few days of her purchase during the data breach; Lawson

"property right" or "independent value" in alleging they "lost control over the value of personal information." Doc. 36 ¶ 88. In response, Plaintiffs deny they brought such a claim. Doc. 57 (Response) at 7. However, Plaintiffs do not explain what meaning other than a property right or independent value of their PII could reasonably be inferred from the allegation in Paragraph 88. Since Plaintiffs admit they did not intend to bring a "property right" or "independent value" claim, the court recommends granting in part the Rule 12(b)(1) motion to partially dismiss Plaintiffs' claims to the extent the Amended Complaint alleges "lost control over the value of personal information." *See* Doc. 36 ¶¶ 88, 137, 182, 184, 238, 240.[4]

Second, Defendant argues Lawson and Baker claim they "overpaid" Chipotle by the implicit amount they believed Chipotle would spend to make the transaction secure. Defendant points to Plaintiffs' allegation of "financial losses related to purchases ... [they] would have never made had they known of Chipotle's careless approach to cybersecurity." Doc. 36 ¶ 88. Defendant cites several cases rejecting the overpayment theory in data breach cases, including *Engl v. Natural Grocers by Vitamin Cottage, Inc.*, No. 15-cv-02129-MSK-NYW, 2016 WL 8578252, at *3 (D. Colo. Sept. 21, 2016). In response, Plaintiffs assert that they do not bring an "overpayment" claim. Doc. 57 (Response) at 7. They argue "if Plaintiffs had known of the lax security they would not

---

alleges his bank informed him within a few weeks of his purchase that he incurred a fraudulent charge. These allegations suffice for traceability. *See, e.g., Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied,* 138 S. Ct. 981 (2018).

[4] If Plaintiffs had defended the independent value allegations, the court would still recommend dismissing. Plaintiffs do not allege they would try to sell their PII; to do so would run contrary to everything they allege. They therefore cannot sue for the monetary value of that information. *See, e.g., Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, No. 15-cv-02129-MSK-NYW, 2016 WL 8578252, at *7 (D. Colo. Sept. 21, 2016) (citing *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015) and *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016)). *See also Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912-13 (7th Cir. 2017); *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 581-82 (E.D.N.Y. 2015), *aff'd,* 589 F. App'x 89 (2d Cir. 2017).

have purchased at Chipotle and so would not have suffered the financial losses they did." *Id.* at 8. *See also* Doc. 36 ¶ 88 (alleging same).

However, Plaintiffs do not address their allegations that part of the monies they paid "were supposed to be used by Chipotle … to pay for the administrative costs of reasonable data privacy and security" (*id.* ¶ 169), they "paid more for that food service than they otherwise would have paid" if they had known Chipotle was not using part of the purchase price for reasonable data security in the transaction (*id.* ¶ 207), and the damages they seek for the portion of their purchase that Chipotle should have spent on data security. *Id.* ¶ 170. Plaintiffs also simultaneously defend their unjust enrichment and California Unfair Competition Law claims as premised on *both* theories that they would not have made the purchases at all, and that a portion of the purchase price was implicitly directed to providing a secure transaction that Defendant did not provide. Doc. 57 (Response) at 17, 23.

The court recommends granting in part the Rule 12(b)(1) motion to the extent Plaintiffs Lawson and Baker allege overpayment for two reasons. First, Plaintiffs argue they did not bring such a claim. This constitutes either an admission or withdrawal of the allegations that assert overpayment. Second, even if Plaintiffs did not intend to admit or withdraw their overpayment allegations for certain claims, they allege overpayment in conclusory fashion. The overpayment theory also fails for the same reasons as in *Engl*. Plaintiffs do not allege facts to plausibly support that part of the purchase price was dedicated to data security. Plaintiffs allege "Chipotle has acknowledged that approximately 70% of its sales are attributable to credit and debit card transactions." Doc. 36 ¶ 23. The court infers that the other 30% of Chipotle's sales are conducted with cash currency. Plaintiffs do not allege they paid higher prices than cash customers. *See, e.g., In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014);

Community Bank, 887 F.3d at 820. Plaintiffs argue that this is irrelevant because cash customers are not part of the proposed class, but they do not address the reasonable inference that a cash customer – who gives no PII to Defendant in a purchase – would pay lower prices than Plaintiffs if their "overpayment" assertion were plausible. Plaintiffs also cite cases in which an overpayment theory survived on unjust enrichment claims: *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016); *In re Anthem, Inc. Data Breach Litig.*, 2016 U.S. Dist. LEXIS 70594, at *167-*175 (N.D. Cal. May 27, 2016); and *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012). *Premera, Anthem* and *Resnick* did not address whether the plaintiffs paid more than cash customers. Those cases in fact did not address whether the defendants even had a significant number of cash customers, considering that all three were providers of health insurance.

This brings the court to Defendant's argument that Lawson and Baker lack standing because they do not allege the actual "time and effort incurred in dealing with [his or her credit/debit card issuer] to address the fraudulent charges actually made on his account or a risk that he might be held responsible for future fraudulent charges." Doc. 43 (Motion) at 8 (quoting *Engl*, 2016 WL 8578252, at *7). Defendants do not take issue with whether the alleged harms are sufficiently particularized[5] or traceable, but only whether Lawson and Baker's harms are sufficiently concrete.

In *Engl*, the court recognizes the two well-established types of injuries that plausibly allege concrete injury in fact: "an actual harm, or … a future harm that is 'certainly impending' or one for which there is 'a substantial risk that the harm will occur.'" *Engl*, 2016 WL 8578252, at *3

[5] The alleged injuries are particularized. Lawson and Baker each allege when he or she made a purchase at Chipotle during the data breach; his or her payment card information was stolen; the number of fraudulent charges attempted or processed on that account; and what they each did after learning of those charges to address, monitor and mitigate the fraud.

(quoting *Clapper*, 133 S. Ct. at 1147). Defendant believes Lawson and Baker argue in their response only the former (actual harm), not the latter (risk of future harm). Doc. 64 (Reply) at 1. But Lawson and Baker allege both existing injuries (Doc. 36 ¶¶ 14, 17) and a risk of future harm. *Id.* ¶¶ 87-104. They also argue both types of harm in their brief, albeit focused primarily on existing injuries. Doc. 57 (Response) at 5 (citing paragraph 102 of the Am. Complaint), 6 n.3 (arguing Lawson's out of pocket expense was justified to mitigate the risk of future harm), 7 (arguing "costs incurred and time spent to… prevent future fraud against them"). The court accordingly considers the allegations of both actual harm and risk of future harm.

1. Alleged Actual Harms

Regarding actual harms, "[a] 'concrete' injury must be '*de facto*'; that is, it must actually exist. … 'Concrete' is not, however, necessarily synonymous with 'tangible.' Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." *Spokeo*, 136 S. Ct. at 1549. "In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles." *Id.* It is "instructive" if the "alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," or if Congress identified the intangible harm as sufficient. *Id.*

In *Spokeo*, plaintiff asserted a "people search engine" violated the Fair Credit Reporting Act by failing to use reasonable methods to ensure accuracy in consumer reports it provides. Plaintiff alleged Spokeo delivered inaccurate information regarding him, such as marital status, age, education and economic status. 136 S. Ct. at 1546. The Court reversed and remanded for the Ninth Circuit to address whether the alleged statutory violation was sufficiently concrete. On remand, the Ninth Circuit found the alleged FCRA violation was in itself a concrete harm, as evinced by the Congressional intent for the FCRA (to protect consumers from inaccurate reports

of personal information that could affect not only their ability to obtain credit but also employment) and the similarity to longstanding reputational and privacy torts. *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1114-15 (9th Cir. 2017), *cert. den'd,* 138 S. Ct. 931 (2018). Plaintiff had standing because he alleged Spokeo's inaccurate report "harmed his employment prospects at a time when he was out of work and that he continues to be unemployed and suffers emotional distress as a consequence." *Id.* at 1111.

Spokeo's focus on whether the inaccuracy of personal information can harm the individual is likewise the focus for standing in the consumer data breach context. In *Engl,* plaintiff's card issuer did not hold him responsible for the unauthorized charge, and he was deprived of the use of his account for only a *de minimis* time. *Engl,* 2016 WL 8578252, at *2. In those circumstances, "[w]ithout the ability to point to time and effort incurred in dealing with Visa to address the fraudulent charges actually made on his account," the plaintiff did not allege an actual harm. *Id.* at *7. In *Weinstein v. Intermountain Healthcare, Inc.*, No. 2:16-cv-00280-DN, 2017 WL 1233829, at *4 (D. Utah Apr. 3, 2017), *appeal dismissed,* No. 17-4071, 2017 WL 5158637 (10th Cir. July 27, 2017), plaintiff alleged defendant violated a statutory requirement to not print the expiration date of his payment card on receipts. He did not, however, allege any misuse of those receipts and thereby failed to allege injury. In *Hammer v. Sam's E., Inc.*, No. 12-cv-2618-CM, 2013 WL 3756573, at *3 (D. Kan. July 16, 2013), plaintiff claimed defendant's website misrepresented its data security but did not allege a security breach or misuse of his information and therefore did not have standing. The Second Circuit similarly found a lack of actual harm from allegations that only payment card information was stolen, the card issuer rejected the attempted fraudulent charges, and a generic, class-wide statement of time or money spent to monitor and address the situation. *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90-91 (2d Cir. 2017).

These cases contrast to consumers who allege the stolen PII was of a type sufficient to enable identity theft (*i.e.*, social security numbers or other personal information required to open new accounts), such as *Hapka v. Carecentrix, Inc.*, Civ. 16-2372-CM, 2016 WL 7336407 (D. Kan. Dec. 19, 2016). In *Hapka*, plaintiff alleged a fraudster obtained PII including social security numbers, birthdates, etc. Shortly after plaintiff was notified of the breach, the IRS notified her that someone had filed a fraudulent tax return using her information. This was sufficient actual harm to support standing.

Here, Ms. Baker alleges:

> On or about March 29, 2017, [she] used her debit card to make a food purchase at … Chipotle ... [in] Riverside, California. … On April 3, 2017, three unauthorized charges were attempted on Plaintiff's debit card. She learned about the attempts via email alerts from her bank, for online purchases of $69.99, $19.99, and $49.99, respectively. The charge of $49.99 went through, but the others were declined. Ultimately, Plaintiff's bank refunded the unauthorized charge.

Doc. 36 ¶ 14 (in relevant part). Much like plaintiff in *Engl* and *Whalen,* Ms. Baker does not allege actual harm: she does not allege she spent time or money addressing the fraudulent charges, whether she was deprived of the use of her account for a time, nor any expenses incurred from the need to (apparently) close and reopen a new account with a new card number.[6]

Mr. Lawson alleges:

> On or around March 28, 2017, … [he] visited [a] Chipotle restaurant … in St. Joseph, Missouri, and purchased food items using his debit card. This debit card is the primary card [he] … uses for daily expenditures because of the cash back rewards benefit. Within a few weeks of this visit, Plaintiff Lawson was contacted by the issuing bank and advised that his debit card had been compromised as a result of the Chipotle Data Breach. The bank informed [him] … that it would be closing the account, opening a new account, and re-issuing a new debit card. Because Plaintiff Lawson had upcoming travel plans, he paid $45 to have the new debit card expedited to him. Unfortunately, despite the attempt to expedite and the money expenditure, a new card did not arrive before he left town. Therefore, Plaintiff Lawson did not have his debit card to use for his travel expenses as he

[6] Ms. Baker does not allege the account in question was closed, but the court infers this from the fact she incurred only three relatively small fraudulent charges on it.

> planned. As a result of having been victimized by the Chipotle Data Breach, Plaintiff Lawson has been required to spend time communicating with his bank regarding his compromised card, account transfer, and replacement card.

Doc. 36 ¶ 17 (in relevant part). Based on this paragraph, Defendant argues Mr. Lawson did not suffer a fraudulent charge. Doc. 43 (Motion) at 9; Doc. 64 (Reply) at 2. Mr. Lawson responds that he did suffer misuse of his card, citing the same paragraph. Doc. 57 (Response) at 4. Although the pleading could be clearer, Mr. Lawson's allegations reasonably infer that his issuing bank went to the trouble of closing and reissuing a new payment card because there was some attempted misuse of his payment card. Defendant is free to pursue the fact issue in discovery, but the court cannot resolve it on a facial challenge to standing.

Mr. Lawson also alleges actual harm in not obtaining the "cash back rewards" on his travel expenses. Defendant argues this is insufficient, citing *Engl*, 2016 WL 8578096, at *6. But in *Engl*, plaintiff alleged only that he lacked the use of his card for several days, not that he thereby lost cash back rewards. Defendant does not explain why the court should consider cash back rewards as having no monetary value as a matter of law. *Cf., Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 969 (7th Cir. 2016) ("Kosner also alleges that he was unable to accrue points on his debit card while he was waiting for a replacement. If that loss has any monetary value (a question on which we take no position), it would be compensable").

Mr. Lawson also alleges actual harm in time spent addressing the theft of his payment card information and new card issuance. Defendant notes that unlike the other named Plaintiffs, Mr. Lawson alleges his lost time generally instead of specifying the duration, inferring he spent only *de minimis* time. Doc. 64 (Reply) at 2. Defendant cites *Engl* on this point, but in that case, plaintiff did not allege he spent any time at all. Nor do Defendant's other cited cases support its argument. In *Randolph v. ING Life Ins.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007), plaintiffs alleged their personal

information was contained on a laptop stolen from a home. Because they did not allege the laptop was stolen to obtain that information, and alleged no attempts to misuse it, the court held the time and inconvenience plaintiffs incurred to monitor their credit was inadequate to allege standing. In *Whalen,* the court found a generic, class-wide allegation of lost time did not suffice. 689 F. App'x at 91. To the extent *Whalen* could be read as requiring consumers to plead with specificity the amount of time they lost, this would run contrary to the pleading standard. *Pueblo of Jemez,* 790 F.3d at 1172 ("Under Rule 8, specific facts are not necessary; the statement need only give the defendant fair notice of what the ... claim is and the ground upon which it rests."). At this phase, the court gives reasonable inferences in Mr. Lawson's favor. *Sanchez v. Hartley,* 810 F.3d 750, 754 (10th Cir. 2016). Defendant is free to pursue the fact issue, but the court cannot resolve it on this motion.

Defendant argues Mr. Lawson's out of pocket expense was "self-inflicted," in the sense that no one required him to expedite delivery of his new card. It is true "self-imposed risk-mitigation costs, when "incurred in response to a speculative threat" do not suffice for standing. *Attias v. Carefirst, Inc.,* 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied,* 138 S. Ct. 981 (2018) (quoting *Clapper*, 568 U.S. at 416-17). But Mr. Lawson's allegations infer that he incurred the expediting fee in the attempt to not lose the cash back rewards he expected on his travel expenses. This plausibly alleges an actual harm for standing. Thus, as to Mr. Lawson, the court sees no need to reach whether he also alleges a risk of future harm. The court proceeds to that question only as to Ms. Baker.

2. Alleged Risk of Future Harm

In addition to harms that are actual and existing, a harm that is "imminent, not 'conjectural' or 'hypothetical'" also suffices for standing. *Lujan*, 504 U.S. at 560. "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk'

that the harm will occur." *Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2334, 2341 (2014) (internal quotation marks omitted, quoting *Clapper,* 568 U.S. at 414, n.5). The Court has not decided whether a "substantial risk" of future harm is different from a "certainly impending" harm (*see, e.g., In re SuperValu, Inc.,* 870 F.3d 763, 769, n.3 (8th Cir. 2017)), but both concepts require something more than an "objectively reasonable likelihood" of future harm. *Clapper*, 568 U.S. at 410.

> Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending. ... . Thus, we have repeatedly reiterated that threatened injury must be *certainly impending* to constitute injury in fact, and that [a]llegations of *possible* future injury are not sufficient.

Id. at 409 (emphasis original, internal quotation marks omitted). In *Clapper*, plaintiffs lacked standing because their alleged risk of future harm – of having their private communications with international persons intercepted under the Foreign Intelligence Surveillance Act – depended on an attenuated chain of causation. In short, "'some day' speculations are insufficient." *Colo. Outfitters Ass'n v. Hickenlooper*, 823 F.3d 537, 551 (10th Cir. 2016).

Engl reviewed the then-extant consumer data breach cases and concluded in order for a consumer to allege a sufficient risk of future harm from a data breach, the consumer must allege "(i) his or her credit card or other financial or personal data was exposed to hackers in a data breach, and (ii) that there is reason to believe that the hackers or others are making actual fraudulent use of the purloined data." *Engl,* 2016 WL 8578252 at *6. Plaintiff in that case alleged actual misuse of his stolen credit card number, and the court recognized in "ordinary circumstances," that would be sufficient to plausibly allege injury. *Id.* However, plaintiff's other allegations showed there was no ongoing potential for harm (the compromised account was closed, he was reimbursed,

and only his payment card information was stolen), so plaintiff's assertions regarding future harm were speculative. *Id.*

Post-*Engl*, several circuit courts have addressed the issue of future harm from data breaches. *See, e.g.*, Joseph F. Yenouskas, Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, 73 Bus. Law. 475 (Spring 2018) (collecting cases); *SuperValu*, 870 F.3d at 769 (also collecting cases), *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, No. 17-1506, 2018 WL 2927626, at *5-6 (4th Cir. June 12, 2018). As the Eighth Circuit notes, "[t]hese cases came to differing conclusions on the question of standing. We need not reconcile this out-of-circuit precedent because the cases ultimately turned on the substance of the allegations before each court." *SuperValu*, 870 F.3d at 769. That is, a risk of future identity theft is sufficient for standing only if the data breach exposed the types of PII that can enable identity theft.

For instance, in *SuperValu*, consumers brought a putative class action after their payment card information was stolen, alleging

> The hackers installed malicious software on defendants' network that allowed them to gain access to the payment card information of defendants' customers (hereinafter, Card Information), including their names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs). By harvesting the data on the network, the hackers stole customers' Card Information.

SuperValu, 870 F.3d at 766. Those allegations are quite similar to Plaintiffs' allegations here:

> When Chipotle's customers pay using credit or debit cards, Chipotle collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Chipotle stores the Customer Data in its POS system and transmits this information to a third party for completion of the payment.
>
> Beginning on or about March 24, 2017, hackers utilizing malicious software accessed the point-of-sale ("POS") systems at Chipotle and Pizzeria Locale

> locations throughout the United States and stole copies of customers' Card Information and other personal information. The software used in the attack was a malware strain designed to siphon data from cards when they are swiped at infected POS systems.

Doc. 36 ¶¶ 24-25. Much like Plaintiffs in this case (doc. 36 ¶¶ 91-95), plaintiffs in *SuperValu* alleged the breach of their payment card information caused a substantial risk of future identity theft. 870 F.3d at 770. They cited the same Government Accounting Office ("GAO") report that Plaintiffs cite here. Doc. 36 at 33, n. 24 (citing GAO 07-737, *Report to Congressional Requesters*, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 33 (June 2007), *available at* <http://www.gao.gov/new.items/d07737.pdf>. But as the Eighth Circuit notes, the GAO report lends no support to allegations of future harm, if only payment card information is breached.

> [T]he allegedly stolen Card Information does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers. As the GAO report points out, compromised credit or debit card information, like the Card Information here, "generally cannot be used alone to open unauthorized new accounts." *Id.* at 30 ... As such, ... there is little to no risk that anyone will use the Card Information stolen in these data breaches to open unauthorized accounts in the plaintiffs' names.

SuperValu, 870 F.3d at 770.[7] *See also Whalen*, 689 F. App'x at 90; *Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 864 (S.D. Ind. 2016), *appeal dismissed* (7th Cir. May 16, 2016). Plaintiffs also do not point to any historical practice or Congressional intent finding a "certainly impending" harm or "substantial risk" thereof when payment card information is stolen, once the compromised account is closed.

---

[7] Here, Plaintiffs also cite several websites and a study by the Department of Justice's Bureau of Justice Statistics regarding how much time consumers spend addressing the misuse of stolen personal information. Doc. 36 ¶ 96; *Victims of Identity Theft, 2012* (Dec. 2013) at 10, *available at* <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited June 22, 2018). But Plaintiffs do not appear to allege these studies support the assertion that theft of payment card information increases the risk of future identity theft.

In this case, there is a fact issue regarding whether more than just Ms. Baker's name and credit card account number were stolen. Plaintiffs allege the stolen information *includes* "cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards." Doc. 36 ¶¶ 24-25. *See also Id.* ¶ 28 (alleging Chipotle confirmed a breach involving "track data" *including* those same categories of information "read from the magnetic stripe"). Plaintiffs allege Chipotle has not said precisely what types of information were actually taken. *Id.* ¶¶ 32-33. Plaintiffs allege in other data breaches, fraudsters stole personal information regarding far more customers than those whose payment card information they stole in the breach, or combine the PII obtained from multiple sources. *Id.* ¶¶ 44-45. On the other hand, the only named Plaintiff to allege fraudulent accounts were opened in her name is Ms. Fowler, and she alleges that occurred two months after the misuse of her stolen card information. *Id.* ¶ 15. However, identity theft can take years to surface. *Id.* ¶ 94.

In short, the court will infer from the allegations that additional personal information was taken in the Chipotle breach that could enable fraudulent accounts to be opened in Ms. Baker's name, or other benefits to be taken fraudulently in her name. This is the "ordinary circumstance" recognized in *Engl*. Because Ms. Baker alleges she suffered actual fraudulent charges on her account, and she does not know for certain whether PII beyond her payment card information was stolen, she plausibly alleges a certainly impending harm or substantial risk thereof. Defendant is of course free to pursue the fact issues regarding Ms. Baker's standing.

In sum, the court recommends denying the Rule 12(b)(1) motion except as to the allegations of "lost control over the value of personal information" and overpayment.

B. Failure to State a Claim

The court turns to Defendant's motion to dismiss for failure to state a claim under Rule 12(b)(6). A court may dismiss a complaint for "failure to state a claim upon which relief can be

granted." *See* Fed. R. Civ. P. 12(b)(6). In deciding a motion under Rule 12(b)(6), we "assume the truth of all well-pleaded facts in the complaint, and draw all reasonable inferences therefrom in the light most favorable to the plaintiffs." *W. Watersheds Project v. Michael*, 869 F.3d 1189, 1193 (10th Cir. 2017) (internal quotation marks omitted). However, a plaintiff may not rely on mere labels or legal conclusions, "and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

To withstand a motion to dismiss, a "complaint must allege facts that, if true, state a claim to relief that is plausible on its face. A claim is facially plausible when the allegations give rise to a reasonable inference that the defendant is liable." *Big Cats of Serenity Springs, Inc. v. Rhodes*, 843 F.3d 853, 858 (10th Cir. 2016) (internal quotation marks omitted). *See also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Once plaintiff pleads sufficient facts to make the claim plausible, "a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of [the alleged] facts is improbable, and that a recovery is very remote and unlikely." *Sanchez*, 810 F.3d at 756 (internal quotation marks omitted, quoting *Twombly*, 550 U.S. at 556).

Generally, a court considers only the contents of the complaint when ruling on a Rule 12(b)(6) motion. *Gee v. Pacheco*, 627 F.3d 1178, 1186 (10th Cir. 2010). Exceptions to this general rule include: documents incorporated by reference in the complaint; documents referred to in and central to the complaint, when no party disputes their authenticity; and "matters of which a court may take judicial notice." *Id.* (quoting *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007)). If a plaintiff does not incorporate by reference or attach a document to its complaint, a defendant may submit an indisputably authentic copy which the court may consider in ruling on the motion without converting it to summary judgment. *GFF Corp. v. Ass'd Wholesale Grocers, Inc.*, 130 F.3d 1381, 1384 (10th Cir. 1997).

1. Negligence Claim (Count 1)

Defendant argues the negligence claim is barred by the economic loss doctrine. As negligence is a matter of state law, the court must first address whether choice-of-law analysis is required. Defendant argues this is unnecessary because in its view these claims fail under the law of all five states in question: the forum state (Colorado) and each named Plaintiff's home state (Arizona, California, Illinois and Missouri). In response, Plaintiffs argue their claims survive under all five states' laws and do not address whether a choice of law is necessary.[8]

"When more than one body of law may apply to a claim, the Court need not choose which body of law to apply unless there is an outcome determinative conflict between the potentially applicable bodies of law." *SELCO Cmty. Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1292 (D. Colo. 2017), *appeal dismissed*, No. 17-1289, 2017 WL 7668565 (10th Cir. Nov. 20, 2017) (internal quotation marks omitted). *See also Security Serv. Fed. Credit Union v. First Am. Mortg. Funding, LLC*, 861 F. Supp. 2d 1256, 1264 (D. Colo. 2012), *recon. den'd*, 906 F. Supp. 2d 1108 (D. Colo. 2012). The "economic loss doctrine" is recognized in the five states at issue, but as will be seen there are outcome-determinative differences between Colorado on the one hand and Arizona and California on the other.

Arizona (Plaintiff Gordon). Arizona recognizes a "narrow version" of the economic loss doctrine. *Flagstaff Affordable Hous. Ltd. P'ship v. Design All., Inc.*, 223 P.3d 664, 668 (Ariz. 2010). Arizona first limits the doctrine to contracting parties. *Flagstaff*, 223 P.3d at 667. "[A]bsent any contract between the parties," it does not apply to tort claims. *Id.* Even as between contracting parties,

[8] The court appreciates brevity in briefing, but in this instance the parties attempted to cover complex areas of law – such as the economic loss doctrine – in only a few paragraphs per state, and neither side fully briefed the choice of law issue. For efficiency's sake the court recommends permitting them to do so on any objections to this recommendation.

> [r]ather than adopting the majority rule as a blanket disallowance of tort recovery for economic losses, we think the better rule is one which examines the loss in light of the nature of the defect that caused it, the manner in which it occurred, and the nature of any other contemporaneous losses.

Salt River Project Agric. Improvement & Power Dist. v. Westinghouse Elec. Corp., 694 P.2d 198, 209 (Ariz. 1984).

> Under *Salt River,* the economic nature of the loss is only one factor in a three-part test to determine whether tort remedies will be available: a court must also consider whether the defect was "unreasonably dangerous" and whether the loss occurred in a "sudden, accidental manner." ... When these factors are present, *Salt River* allows a plaintiff to recover in tort for purely economic loss.

Flagstaff, 223 P.3d at 668 (quoting *Salt River,* 694 P.2d at 209).

Thus "[t]he economic loss doctrine may vary in its application depending on context-specific policy considerations. To determine whether the doctrine should apply..., we must consider the underlying policies of tort and contract law" in the case-specific context. *Id.* at 669. "The principal function of the economic loss doctrine, in our view, is to encourage private ordering of economic relationships and to uphold the expectations of the parties by limiting a plaintiff to contractual remedies for loss of the benefit of the bargain. These concerns are not implicated when the plaintiff lacks privity and cannot pursue contractual remedies." *Id.* at 671. *See also Sullivan v. Pulte Home Corp.*, 306 P.3d 1, 3 (Ariz. 2013) ("encourage the private ordering of economic relationships, protect the expectations of contracting parties, ensure the adequacy of contractual remedies, and promote accident-deterrence and loss-spreading.").

To date, the Arizona Supreme Court has recognized the economic loss doctrine only in product liability and construction cases that involved contracting parties. *Flagstaff,* 223 P.3d at 665. It has declined to extend the doctrine to a non-contracting party's construction claim, regardless that the party at one time "had a possible contractual remedy under an implied warranty claim. Such a remedy was imposed as a matter of Arizona's common law; it did not result from

any opportunity the [subsequent homeowners] had to negotiate with [the defendant homebuilder] over remedies." *Sullivan*, 306 P.3d at 3.

The District of Arizona has predicted the Arizona Supreme Court would extend the doctrine to claims regarding credit card payment processing between two sophisticated contracting entities. *TSYS Acquiring Sols., LLC. v. Elec. Payment Sys., LLC*, No. CV10-1060 PHX, 2010 WL 3882518, at *2 (D. Ariz. Sept. 29, 2010) (the defendant did "not argue that it lacked the sophistication to assess risks, negotiate the contract, or prospectively identify remedies for breach. Nor does it allege that breach of the contract was unforeseeable"). The court also predicts Arizona would extend the doctrine to claims regarding damages from underground pollution that was the subject of contract between two sophisticated parties. *Greyhound Lines Inc. v. Viad Corp.*, No. CV-15-01820-PHX-DGC, 2016 WL 6833938, at *8 (D. Ariz. Nov. 21, 2016).

However, the District of Arizona has predicted the state would not extend the economic loss doctrine in two data breach cases. *Cumis Ins. Society, Inc. v. Merrick Bank Corp.*, No. CV-07-374-TUC-CKJ, 2008 WL 4277877 (D. Ariz. Sept. 18, 2008); *In re Banner Health Data Breach Litig.*, No. CV-16-02696-PHX-SRB, 2017 WL 6763548 (D. Ariz. Dec. 20, 2017). In *Cumis*, plaintiff was the insurer of credit unions whose customers had their payment card information stolen from a card processor's computers in a data breach. The insurer claimed one defendant (Merrick) had contracted (it is unclear with whom, but not with the insurer) to guarantee a processor's compliance with PCI standards; the other defendant (Savvis) contracted (apparently with Merrick or the processor) to certify the processor's computer systems complied with PCI DSS. The insurer alleged Savvis did so faultily, and this led to the processor's data breach. The court analyzed the facts under *Salt River*:

> The alleged breach of the contract itself did not cause the loss—although the data security breach could not have occurred without [it] .... The alleged breach of

> contract presented a real danger of harm to persons or property because it, allegedly, permitted the data security breach. The data security breach is comparable to a tortious "accident" and the damages are of a type that caused economic harm to persons or entities. ... The Court finds that the *Salt River* factors are present and, therefore, ... [d]ismissal of the tort claims based on the economic loss rule is not appropriate.

Cumis, 2008 WL 4277877, at *8.

Banner Health is a data breach case brought by consumers. The court gave two reasons for finding the doctrine did not apply to the consumers' negligence claims. First, Arizona has not extended the doctrine beyond construction defects and product liability. Second, although plaintiffs had express contracts with defendant, none of the contracts obligated defendant to do anything with respect to data security that it did not already have statutory duties to do anyway. *Banner Health*, 2017 WL 6763548, at *8. The contracts either failed for lack of consideration or did not address data security. The court concluded that "Plaintiffs have as of yet failed to allege adequately the existence of a contract governing data security between the parties, making it inappropriate to dismiss their claim for negligence at this stage ... based on a rule designed solely for the purpose of distinguishing contractual and tort duties. *Id.*

Defendant argues *Banner Health* is misguided because the economic loss rule should apply to the tort claims of any parties who had a "direct relationship." The court is not persuaded. Arizona does not focus on whether the parties merely had a "direct relationship;" the Arizona Supreme Court expressly limits the doctrine to "contracting" parties and asks (among other things) whether the party had an opportunity to negotiate the terms and remedies at issue, such that the parties' contractual expectations should be enforced. *See, e.g., Flagstaff*, 223 P.3d at 669;[9]

[9] "Construction-related contracts often are negotiated between the parties on a project-specific basis and have detailed provisions allocating risks of loss and specifying remedies. In this context, allowing tort claims poses a greater danger of undermining the policy concerns of contract law." *Flagstaff*, 223 P.3d at 669.

Sullivan, 306 P.3d at 3 (the doctrine requires "an agreement between the parties allocating economic risks," internal quotation marks omitted). Parties can have a "direct" relationship without necessarily having the opportunity to negotiate and allocate risks. *See also Deepwater Divers, Inc. v. Wells Fargo Ins. Servs. USA, Inc.*, No. 1 CA-CV 13-0518, 2015 WL 4020877, at *4 (Ariz. Ct. App. June 30, 2015), *as amended* (Oct. 5, 2015) (declining to apply economic loss doctrine despite the parties having a direct relationship through an alleged implied contract because "[t]he economic loss doctrine ... applies only when the parties have entered into a contract defining their relationship"); *Barmat v. John & Jane Doe Partners A–D*, 747 P.2d 1218, 1222 (Ariz. 1987) (where an implied contract "does no more than place the parties in a relationship in which the law then imposes certain duties recognized by public policy, the gravamen of the subsequent action for breach is tort, not contract," cited in *Deepwater*).

As in *Cumis* and *Banner*, this court concludes Arizona's economic loss doctrine does not bar Plaintiff Gordon's negligence claims for two reasons. First and foremost, Plaintiffs' claims do not arise in the two contexts (product liability and home construction) in which the Arizona Supreme Court has recognized the doctrine to date. Secondly, Plaintiffs do not allege they expressly contracted or negotiated with Defendant at all, let alone regarding the security of their POS system or their payment card information and remedies for a breach thereof.[10] Plaintiffs allege only an implied contract based on their use of payment card systems and Defendant's implied promise to follow its online privacy policy in its in-store transactions. Doc. 57 (Response) at 14. Elsewhere in its motion, Defendant points to the interrelated PCI contracts as the source of its data security obligations to Plaintiffs, but Defendant does not cite any authority that Arizona would apply the economic loss doctrine based on interrelated contracts. In light of Arizona thus

[10] Although Plaintiffs allege in passing an express contract regarding data security (paragraph 42), they do not allege facts to support such a contract.

far limiting the doctrine to parties in privity, the court declines to extend Arizona's economic loss doctrine to parties with interrelated contracts.[11] In short, if Arizona law applies to Mr. Gordon's negligence claim, the court concludes it is not barred.

California (Plaintiffs Marc and Kristen Mercer, Judy Conard, and Kristin Baker). The California Supreme Court discusses the economic loss doctrine as maintaining a boundary line between tort and contract.

> A person may not ordinarily recover in tort for the breach of duties that merely restate contractual obligations. Instead, [c]ourts will generally enforce the breach of a contractual promise through contract law, except when the actions that constitute the breach violate a social policy that merits the imposition of tort remedies.

Aas v. Superior Court, 12 P.3d 1125, 1135 (Cal. 2000) (internal quotation marks omitted) *superseded by statute on other issue.*

> A consumer should not be charged at the will of the manufacturer with bearing the risk of physical injury when he buys a product on the market. He can, however, be fairly charged with the risk that the product will not match his economic expectations unless the manufacturer agrees that it will. Even in actions for negligence, a manufacturer's liability is limited to damages for physical injuries and there is no recovery for economic loss alone.

Id. (internal quotation marks omitted). "Courts should be careful to apply tort remedies only when the [alleged] conduct in question is so clear in its deviation from socially useful business practices that the effect of enforcing such tort duties will be ... to aid rather than discourage commerce." *Robinson Helicopter Co. v. Dana Corp.,* 102 P.3d 268, 275 (Cal. 2004) (internal quotation marks omitted, finding fraud claim not barred by economic loss rule).

Defendant argues that "[u]nder California law, 'a plaintiff's tort recovery of economic damages is barred unless such damages are accompanied by some form of physical harm (i.e.,

[11] Mr. Gordon does not address any of the above. He instead argues Chipotle's conduct caused a negative impact to his credit score, a reputational harm that in his view is non-economic. Doc. 57 (Response) at 8. The court does not reach this issue for Arizona law.

personal injury or property damage),'" quoting *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 961 (S.D. Cal. 2012). The California Plaintiffs (the Mercers, Conard and Baker) argue their negligence claim is not barred because they had a "special relationship" with Chipotle, citing *J'Aire Corp. v. Gregory*, 598 P.2d 60, 62–63 (Cal. 1979). This exception requires the court to consider six factors:

> (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.

J'Aire, 598 P.2d at 63. "All six factors must be considered by the court and the presence or absence of one factor is not decisive." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 968 (S.D. Cal. 2014) (citing *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605-06 (9th Cir. 2008), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

Defendant argues the special relationship exception is inapplicable because Plaintiffs have a direct relationship with Defendant, *i.e.*, privity. California's leading cases do define this exception in terms of third persons to a contract or transaction. *J'Aire*, 598 P.2d at 64; *Biakanja v. Irving*, 320 P.2d 16, 18 (Cal. 1958). *See also Centinela Freeman Emergency Med. Assocs. v. Health Net of California, Inc.*, 382 P.3d 1116, 1128 (Cal. 2016) (discussing special relationship as an "exceptional duty to third parties"). However, those cases did not address plaintiffs who had a direct relationship with the defendant. In cases presenting plaintiffs in privity with a defendant, some courts do not address whether the privity made the special relationship exception inapplicable on its face. *See, e.g., Sony Gaming*, 903 F. Supp. 2d at 961-62. Other courts address the issue but distinguish between contracts for services as opposed to goods. *See, e.g., In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2018 WL 1243332, at *11 (N.D.

Cal. Mar. 9, 2018) (following *N. Am. Chemical Co. v. Superior Court*, 59 Cal. App. 4th 764, 784–85, 69 Cal. Rptr. 2d 466, 477–78 (1997)); *cf., Resnick v. Hyundai Motor Am., Inc.*, No. CV1600593BROPJWX, 2017 WL 1531192, at *11 (C.D. Cal. Apr. 13, 2017) (quoting cases regarding significance of privity in contracts for goods).[12]

In addition, the cases on which Defendant relies regarding privity involve express contracts. *Resnick*, 2017 WL 1531192, at *11; *Body Jewelz, Inc. v. Valley Forge Ins. Co.*, 241 F. Supp. 3d 1084, 1092–93 (C.D. Cal. 2017). *See also In re Sony Gaming*, 996 F. Supp. 2d at 954 (consumers alleged Sony required them to enter express contract and to provide PII in doing so). Here, Plaintiffs allege only an implied in fact contract. Given the mixed caselaw, the court will assume California's "special relationship" exception is available to Plaintiffs despite their direct purchases from Defendant.

Regarding the first *J'Aire* factor for a special relationship ("extent to which the transaction was intended to affect the plaintiff"), Defendant plainly intended to transact with each Plaintiff, but nothing in the Amended Complaint suggests either side intended these relatively small credit card transactions to significantly affect Plaintiffs. This factor does not significantly weigh in favor of either side. *Cf., Wells Fargo Bank, N.A. v. Renz*, 795 F. Supp. 2d 898, 926 (N.D. Cal. 2011) (a pollution-remediation case cited by Defendant, in which the court noted the claimant's "special relationship" argument would apply equally to any user of the defendant's equipment).

The second factor – foreseeability of harm – weighs in favor of Plaintiffs. Regardless that Plaintiffs' purchases were small, Defendant could easily foresee the harm to Plaintiffs if it did not use reasonable steps to guard its POS systems from fraudsters. Plaintiffs allege Chipotle was aware from highly publicized data breaches at other restaurants (and other large retailers in the

[12] *Aas* appears to have rejected the goods vs. services distinction. *Aas*, 12 P.3d at 1135–36. *See also Sony Gaming*, 903 F. Supp. 2d at 961-62 (noting Ninth Circuit rejected such a distinction).

United States) of the threat to its POS systems for malware infection. They allege Chipotle knew the PCI's upgrade to chip-readers was intended to address the malware threat, and Chipotle allegedly decided to place a higher priority on speed than security.

The third factor – certainty Plaintiffs suffered injury – each of the California Plaintiffs alleges they suffered fraudulent charges on the credit or debit accounts that they used to make purchases at Chipotle during the time of the data breach. This weighs in Plaintiff's favor, as does the fourth factor, closeness of connection. Each of the California Plaintiffs alleges the fraudulent charges occurred relatively soon after they made those purchases – between a few days and two months. The fifth factor for moral blame attached to Chipotle's conduct is not high. Chipotle allegedly knew it was not taking all steps the PCI DSS required for better securing payment card information, but Chipotle did not allegedly aid the fraudsters and is itself also a victim in a sense. This factor does not weigh in favor of either side. The sixth factor – policy of preventing future harm – at least when weighed at the Rule 12 phase, giving Plaintiffs the reasonable inferences from their allegations, tort remedies may have greater effect than implied contract remedies, in ensuring Chipotle (and other vendors) take reasonable steps to ensure consumers' payment information. Overall, the *J'Aire* factors weigh in favor of excepting Plaintiffs' negligence claim from California's economic loss doctrine.

This conclusion is consistent with other data breach cases that address the "special relationship" issue with sufficient analysis to permit comparison of the fact allegations. For instance, Defendant relies on *Sony Gaming*, a data breach case brought by consumers. The plaintiffs there alleged Sony was aware of data security vulnerabilities and failed to take steps to address them, but did not allege they suffered actual attempts of identity theft or fraudulent charges. The uncertainty of injury and lack of close connection weighed heavily against plaintiffs.

Although a few of the factors weighed in favor of plaintiffs, overall the court concluded that because they did not allege any relationship with the breached vendor "beyond those envisioned in everyday consumer transactions," the exception did not apply. 996 F. Supp. 2d at 969. Defendant also cites *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016), another consumer data breach case. But the court simply noted plaintiff "puts forth no facts to demonstrate that a special relationship existed between him and Defendants." *Dugas* does not provide enough reasoning regarding the fact allegations in that case to be persuasive.

Plaintiffs cite *In re Experian Data Breach Litigation*, No. SACV 15-1592 AG, 2016 WL 7973595, at *8 (C.D. Cal. Dec. 29, 2016), but *Experian* did not address California's special relationship exception. The court finds the Northern District of California's recent decision in *Yahoo* more persuasive here. That case apparently involves an express contract, but otherwise the allegations are similar to Plaintiffs' allegations here: that they provided PII to defendant with the understanding it would reasonably protect that information and promptly inform them of breaches, and defendant knew they in fact did not have adequate data security and did not have the technology to promptly discovery breaches. The court found these facts sufficient to allege a special relationship under *J'Aire*, and thus declined to find the negligence and deceit by concealment claims barred by the economic loss doctrine. *In re Yahoo!*, 2018 WL 1243332, at *11–12 (citing *In re Adobe Sys., Inc. Privacy Litig.*, 66 F.Supp.3d 1197, 1224 (N.D. Cal. 2014)). In all, the court concludes the *J'Aire* factors weigh in favor of Plaintiffs and they meet the special relationship exception. If California law applies to the California Plaintiffs' negligence claim, the claim is not barred by the economic loss doctrine.[13]

[13] The Mercers also argue they suffered reputational harm and that this is a non-economic injury. The court does not reach this issue.

Illinois (Ms. Fowler). Defendant argues Ms. Fowler's negligence claim fails under Illinois law for lack of a common law duty to safeguard consumers' credit card information. Defendant cites *Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 28 (Ill. App. 2010), *appeal denied*, 949 N.E.2d 657 (2011) (table decision). Plaintiffs argue Illinois law in opposing Defendant's other arguments regarding this claim, but they do not address this issue. *Cooney* notes the Illinois legislature enacted a data breach statute that only requires breached entities to give notice to consumers. 815 ILCS 530/10 (West 2006). The statute does not provide a private right of action or damages. The court held:

> While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review.

Cooney, 943 N.E.2d at 29. The Illinois Supreme Court has not ruled on the issue. Absent such a ruling, "federal courts turn to decisions of the Illinois Appellate Court, which are accorded 'great weight.'" *Landale Signs & Neon, Ltd. v. Runnion Equip. Co.*, 274 F. Supp. 3d 787, 791 (N.D. Ill. 2017). "There is … no 'indication' that the Illinois Supreme Court would deviate from *Cooney*'s holding; indeed, plaintiffs' appeal in *Cooney* was denied." *Id.* As the Seventh Circuit held recently, *Cooney*

> reads as a more general statement that no duty to safeguard personal information existed, regardless of the kind of loss. … Nothing in the *Cooney* analysis indicates that retail merchants like Schnucks should or would be treated differently than the former employer and contractor at issue there. In the absence of some other reason why the Illinois Supreme Court would likely disagree with the *Cooney* analysis … we predict that the state court would not impose the common law data security duty the plaintiff banks call for here.

Cmty. Bank of Trenton v. Schnuck Markets, Inc., 887 F.3d 803, 816 (7th Cir. 2018) (note omitted). *See also USAA Fed. Sav. Bank v. PLS Fin. Servs., Inc.*, 260 F. Supp. 3d 965, 970 (N.D. Ill. 2017) (dismissing negligence claim brought under Illinois law with prejudice); *In re SuperValu, Inc.*,

Customer Data Sec. Breach Litig., No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *14 (D. Minn. Mar. 7, 2018) (same).

Plaintiffs cite a data breach case in which an Illinois negligence claim survived a motion to dismiss: *In re Experian Data Breach Litig.*, No. SACV15-1592-AGD-FMX, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016). But in allowing the case to proceed, the *Experian* court did not address defendant's argument that it "didn't owe the Illinois Plaintiffs a duty." *Id.* Without reasoning on the issue, the case is not persuasive. As such, under Illinois law the negligence claim should be dismissed for lack of a common law duty.[14]

Missouri (Mr. Lawson). Defendant argues that in Missouri, "[t]he economic loss doctrine prohibits a party from seeking to recover in tort for economic losses that are contractual in nature." *Graham Constr. Servs. v. Hammer & Steel Inc.*, 755 F.3d 611, 616 (8th Cir. 2014). Losses are "contractual in nature" unless "there is personal injury, damage to property other than that sold, or destruction of the property sold due to some violent occurrence." *Captiva Lake Invs., LLC v. Ameristructure, Inc.*, 436 S.W.3d 619, 628 (Mo. Ct. App. 2014). Mr. Lawson did not allege such an injury. Defendant further argues Missouri recognizes only a few exceptions for "fiduciary relationships, professional malpractice, and breach of a public duty," citing *Dannix Painting, LLC v. Sherwin-Williams Co.*, 732 F.3d 902, 905 (8th Cir. 2013). Defendant argues Mr. Lawson does not allege facts to support those exceptions and therefore his claim is barred.

In response, Mr. Lawson relies on a "special relationship" exception. He asserts this exception applies where "the nature of the tort action asserted . . . arises from the rendering of services to be provided by a contract and that the conduct of [the defendant] is the basis of the

[14] The same would result under Colorado law. Plaintiffs were on notice to brief the duty issue under Colorado law (its economic loss doctrine focuses primarily on the duty), and they do not cite any authorities for such a duty under Colorado law.

allegations and not the state of a home or product," quoting *Autry Morlan Chevrolet, Cadillac, Inc. v. RJF Agencies, Inc.*, 332 S.W.3d 184, 194 (Mo. Ct. App. 2010). Mr. Lawson argues the basis of his claim is "not the quality or state of the good bargained for, but Defendant's conduct in failing to adequately safeguard Plaintiff's personal information" and therefore the claim is not barred. *Autry Morlan* addressed a contract action in which the defendant owed a fiduciary duty; specifically, a contract between a principal and a broker acting as its agent. 332 S.W.3d at 193-94. *See also Dannix Painting, LLC v. Sherwin-Williams Co.*, 732 F.3d 902, 905 (8th Cir. 2013) (limiting *Autry Morlan* to contracts in a fiduciary relationship). Mr. Lawson does not allege Chipotle owed a fiduciary duty to him. Missouri law would bar his negligence claim under the economic loss doctrine.

Colorado. Colorado is the forum state and where Defendant is or was headquartered at the time of the data breach. No named Plaintiffs reside here. In Colorado law,

> a party suffering only economic loss from the breach of an express or implied contractual duty may not assert a tort claim for such a breach absent an independent duty of care under tort law. Economic loss is defined generally as damages other than physical harm to persons or property.

Town of Alma v. AZCO Const., Inc., 10 P.3d 1256, 1264 (Colo. 2000) (note omitted).

> The essential difference between a tort obligation and a contract obligation is the source of the parties' duties.... Contract obligations arise from promises the parties have made to each other, while tort obligations generally arise from duties imposed by law to protect citizens from risk of physical harm or damage to their personal property.

BRW, Inc. v. Dufficy & Sons, Inc., 99 P.3d 66, 72 (Colo. 2004).

The court is to determine the source of the duty alleged to be breached - contractual or tort - by weighing "(1) whether the relief sought is the same; (2) whether there is a recognized common law duty in tort; and (3) whether the tort duty differs from the contractual duty." *Electrology Lab., Inc. v. Kunze*, 169 F. Supp. 3d 1119, 1152 (D. Colo. 2016) (citing *Town of Alma*,

10 P.3d at 1263). In this case, Plaintiffs allege an implied in fact contract for Defendant to use reasonable security measures to protect their PII in its possession. Plaintiffs seek the same relief for that claim as for their negligence claim. Doc. 36 Counts I, IV. Plaintiffs argue "the duties of care being claimed here exist entirely independent of a contract," but they cite no Colorado authority in support. Plaintiffs do not cite any Colorado authorities to support Defendant had an independent duty to safeguard PII.

Even if Plaintiffs had briefed support for the tort duty they presume in the Amended Complaint, they have alleged the same duty under their implied contract. For both claims, Plaintiffs allege the same duty to take reasonable measures to protect their PII that they locate in the PCI "rules and standards" or "operating regulations" for merchants. Doc. 36 ¶¶ 57-70, 78; Count I (negligence) ¶ 116 (incorporating all previous allegations), ¶ 120 ("industry standards and requirements"), 122 (same); Count IV (implied contract) ¶¶ 153 (incorporating all previous allegations), 156 ("industry standards"), 158 (same). In their brief, Plaintiffs argue they do not allege the PCI data security standards as the source of the duty to safeguard their information, but only allege Defendant's failure to meet those standards is evidence of the breach of an independent duty. Doc. 57 (Response at 11-12). But again, Plaintiffs do not brief any Colorado law (or in fact, of any of the five states at issue) that would recognize merchants have an independent duty to safeguard consumers' PII. Moreover, Plaintiffs ignore that they allege one of the PCI standards (EVM technology) as a specific standard Chipotle should have followed and that its decision not to do so enabled the data breach.

This leads to a further difficulty in Plaintiffs' allegations. Plaintiffs allege Defendant was required to follow PCI standards, rules and operating regulations as a "member[] of the payment card industry." Doc. 36 ¶ 78. To the extent the Amended Complaint attempts to allege the PCI

data security standards as though they were the equivalent of industry safety standards or regulatory requirements, this is not plausible. Other allegations show the PCI "industry standards" were contractual: "Under Card Operating Regulations, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, *agree* to be liable for damages resulting from any data breaches." Doc. 36 ¶ 70 (emphasis added).

Under Colorado law, the interrelated PCI contracts allegedly require Chipotle to comply with PCI data security measures and thus suffice to bar the negligence claim – regardless that Plaintiffs are not parties to most of those contracts. *BRW*, 99 P.3d at 74; *SELCO*, 267 F. Supp. 3d at 1296. Plaintiffs emphasize they are not parties to any of the PCI contracts, but each Plaintiff alleges he or she had a relationship with the bank or credit card company who issued their payment cards. Plaintiffs do not allege those relationships are express contracts, but this is a reasonable inference from the allegations. Plaintiffs' implied contract claim is also alleged so broadly and non-specifically, it arguably encompasses a theory that by accepting Plaintiffs' payment cards, Chipotle impliedly agreed with Plaintiffs to comply with its obligations under PCI contracts, including the data security standards therein. Doc. 36, Count 4.[15]

Plaintiffs argue they had no opportunity to bargain and define terms with Chipotle, citing *SELCO* and *BRW*. Yet those very cases applied the economic loss doctrine regardless that plaintiffs did not have the ability to negotiate terms with the defendant, and regardless that the contract may have only memorialized a duty from tort law. *SELCO*, 267 F. Supp. 3d at 1295-96

[15] Plaintiffs do not argue an implied contract based on the inter-related PCI contracts, and their response strongly suggests they would disclaim it. For instance, Plaintiffs argue those contracts do not provide a complete remedy to them. The court does not reach that factual issue.

(citing *inter alia BRW,* 99 P.3d at 74). This is because Colorado law generally deems individuals free to not enter contractual relationships if they wish to negotiate and are not able to do so.[16]

On the other hand, *BRW* and *SELCO* refer to "commercial parties," and *Town of Alma* reasons that the "principle that parties must be able to confidently allocate their risks and costs in a bargaining situation underlies the necessity for the economic loss rule." 10 P.3d at 1261. Plaintiffs are instead individual consumers, albeit purporting to represent large classes of other individuals. But *Town of Alma* involved several individual landowner plaintiffs who did not directly contract or bargain with anyone regarding the public plumbing work that they alleged resulted in their damages; the court nonetheless held the landowners' negligence claims were barred by the town's contract with defendant. This is somewhat akin to the situation here, in which Chipotle contracted with PCI financial institutions and card brands, and Plaintiffs claim damages from its failure to implement the security measures that those contracts required.

Most importantly, Plaintiffs have not pointed the court to any authority that would justify making an exception to *Town of Alma* and *BRW* based on the independent duty they assume merchants owe to consumers to safeguard their PII. For instance, in *A.C. Excavating v. Yacht Club II Homeowners Ass'n, Inc.,* 114 P.3d 862, 863–64 (Colo. 2005), the court declined to apply the economic loss doctrine to homeowners' negligence claims against subcontractors because the subcontractors owed an independent duty in home construction. *Id.* at 863-64. But the court did so only after discussing at length several Colorado cases that established the independent duty. Plaintiffs have not offered any authority for the court to find an independent duty here.

[16] In Colorado, the doctrine applies to implied contracts. *Town of Alma,* 10 P.3d at 1264. Although implied in fact contracts require an offer and assent, they do not necessarily require negotiations in the sense Plaintiffs use here.

Plaintiffs would circumvent these issues by arguing they suffered reputational harm, which they contend is a non-economic injury and thus their claim is not subject to the economic loss doctrine. Doc. 57 (Response) at 11 (citing Doc. 36 ¶¶ 10, 13, 15-16). It is far from clear that each named Plaintiff alleges a reputational harm, but the court will assume without deciding that they do. Plaintiffs cite *James v. Coors Brewing Co.*, 73 F. Supp. 2d 1250, 1253 (D. Colo. 1999). *James* does not address the economic loss doctrine; it construes Colorado's statutory cap on non-economic damages, C.R.S. § 13–21–102.5(2)(b). For purposes of the economic loss doctrine, the Colorado Supreme Court instead defines economic loss as "damages other than physical harm to persons or property." *Town of Alma,* 10 P.3d at 1264. Harm to one's reputation is not physical harm to person or property. As such, for purposes of Colorado's economic loss doctrine, reputational harm is an economic loss.[17]

Even if *James* were apposite here, the court held the non-economic damages statute encompassed reputational harm only "absent evidence of pecuniary harm." *Id.* Plaintiffs do not allege facts to support their reputations were harmed in a non-pecuniary fashion. Some of the named Plaintiffs allege only time and money spent addressing the theft of their card information; others allege fraudulent charges and false reports to their credit lowered their credit scores. One Plaintiff (Mr. Gordon) alleges that his lowered credit score resulted in a higher finance rate on a car loan. Doc. 36 ¶ 11. These are all pecuniary losses. Even if any Plaintiffs alleged the fraudulent credit report changes affected their employment, that too would be pecuniary in nature. *Cf., Warad W., LLC v. Sorin CRM USA Inc.*, 119 F. Supp. 3d 1294, 1306–07 (D. Colo. 2015) (applying Arizona law). In short, in the absence of reasoned argument from Plaintiffs that Colorado would

[17] This definition of economic loss is consistent with Colorado's focus on the source of duty and "not whether the damages are physical or economic." *Town of Alma,* 10 P.3d at 1262 (cited in *Casey v. Colo. Higher Educ. Ins. Benefits All. Tr.*, 310 P.3d 196, 202 (Colo. App. 2012)).

recognize an independent duty in this case, the court concludes Colorado's economic loss doctrine would bar the negligence claim based on the implied contract, the PCI contracts, or both.

In the end then, there are outcome definitive differences for this claim between Colorado on the one hand and on the other Arizona and California. "The Court must apply the choice of law rules of Colorado (the forum state), which follows the Restatement (Second) of Conflict of Laws." *SELCO*, 267 F. Supp. 3d at 1292, n.1 (quoting *Kipling v. State Farm Mut. Auto. Ins. Co.*, 774 F.3d 1306, 1310 (10th Cir. 2014)). In that case, the court found it did not need to reach the choice of law issue, but if it had, Colorado law would govern the negligence claims. *SELCO* found "[s]everal Restatement factors support applying Colorado law over the laws of plaintiffs' home states," namely thatplaintiffs allegeddefendant's tortious conduct (delay in notifying of data breach) occurred at its headquarters in Colorado, andplaintiffs in contrast could have been anywhere when they incurred the alleged injuries of that conduct. Thus the locus of defendant's conduct was given more weight. *Id.* (citing Restatement (Second) of Conflicts § 145 & cmt. e (1971)). The same is true of Plaintiffs' allegations in this case. The court concludes that for Plaintiffs in Arizona and California, Colorado law governs their negligence claims. The court therefore recommends dismissing the negligence claim in Count 1 as to all Plaintiffs.

2. Negligence Per Se Claim (Count 2)

Plaintiffs allege a separate count for negligence per se. Doc. 36, Count 2. For this claim, Plaintiffs locate Defendant's duty to safeguard their PII in Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 and guidelines the FTC promulgated thereunder regarding data security measures. Section 5 prohibits "unfair . . . practices in or affecting commerce." Plaintiffs allege those unfair practices include "as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect Payment Card Data." Doc. 36 ¶ 128. Plaintiffs allege the FTC has issued publications providing guidance on what it considers

reasonable data security measures to avoid violating Section 5, and has issued enforcement orders against companies who failed to use such measures. *Id.* ¶¶ 71-74, 128. Plaintiffs allege Defendant failed to meet the FTC's guidelines. *Id.* ¶ 86; Count 2.[18]

Defendant includes this claim in its argument regarding the economic loss doctrine, but Defendant does not articulate why the analysis would be the same under the five states' laws. In the states that recognize it, the negligence per se claim is based on a duty of care established in a statute or regulation rather than tort law. Defendant did not argue why it apparently assumes the duties established in Section 5 of the FTC Act (or the FTC's data security guidelines thereunder) are not an independent duty sufficient to support the negligence per se claims. *SELCO* reasoned that Section 5 did not support an independent duty and the negligence per se claim was barred, but did so largely because the financial institutions could not show that in their role as credit card issuers they were persons that Section 5 intended to protect. *SELCO,* 267 F. Supp. 3d at 1295, n.3 (Colorado law). But Plaintiffs here are individual consumers and as such are persons whom Section 5 is intended to protect. *See, e.g., F.T.C. v. Accusearch Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009).

Defendant more clearly argues the negligence per se claim fails because the states at issue either do not recognize such a cause of action, or require a statute/regulation that specifies prohibited conduct instead of a general standard of conduct. Defendant is correct California and Illinois do not recognize a separate cause of action for negligence per se. *Quiroz v. Seventh Ave. Ctr.*, 45 Cal. Rptr. 3d 222, 244–45 (Cal. App. 2006); *Abbasi ex rel. Abbasi v. Paraskevoulakos*,

[18] Plaintiffs further allege Chipotle violated "similar state statutes" (doc. 36 ¶ 133), but they do not identify those statutes in the Amended Complaint or their brief.

718 N.E.2d 181, 185 (1999)). In those states, alleged violations of safety statutes are simply evidence of negligence.[19]

Defendant is also correct Arizona, Colorado and Missouri recognize a cause of action for negligence per se only as to violations of statutes that prohibit specific conduct, as opposed to establishing a general standard of conduct. *Griffith v. Valley of Sun Recovery & Adjustment Bureau, Inc.*, 613 P.2d 1283, 1285 (Ariz. Ct. App. 1980); *Winkler v. Shaffer*, 356 P.3d 1020, 1024 (Colo. App. 2015) (citing CJI–Civ. 4th 9:14 (2014), "[i]f a statutory standard of care is a codification of common-law negligence, the negligence per se instruction has no practical effect when given alongside a common-law negligence instruction. In such cases, the court need not give both a common-law negligence instruction and a negligence per se instruction"); *Burns v. Frontier II Props. Ltd. P'ship*, 106 S.W.3d 1, 3 (Mo. Ct. App. 2003) ("Negligence per se arises when the legislature pronounces in a statute what the conduct of a reasonable person must be"); *Cisco v. Mullikin*, No. 4:11 CV 295 RWS, 2012 WL 549504, at *2 (E.D. Mo. Feb. 21, 2012) (statutes that required driving in "careful and prudent manner" and "highest degree of care" did not establish statutory standard of care and therefore did not support negligence per se claim).

Defendant argues Section 5 of the FTC Act does not fit the bill for negligence per se in Arizona, Colorado and Missouri because "unfair … practices in or affecting commerce" is a general standard of conduct, not a specific category of prohibited conduct. Defendant cites *Orkin Exterminating Co. v. F.T.C.*, 849 F.2d 1354, 1367 (11th Cir. 1988) for Section 5's "unfair practice" being an elusive concept. Plaintiffs do not attempt to directly rebut Defendants' cases. They instead respond with a series of federal court cases that allowed negligence per se cases alleging

[19] Because there are outcome-determinative differences between Colorado on the one hand and California and Illinois on the other, Colorado law governs the negligence per se claim for at least the California and Illinois Plaintiffs.

violations of Section 5 of the FTC Act to survive Rule 12: *In re Home Depot, Inc.*, MDL No. 2583, 2016 U.S. Dist. LEXIS 65111, at *30 (N.D. Ga. May 17, 2016); *Bans Pasta, LLC v. Mirko Franchising, LLC,* No. 7:13-cv-00360-JCT, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014); and *First Choice Fed. Credit Union v. Wendy's Co.*, No. 16-506, 2017 U.S. Dist. LEXIS 20754, at *13 (W.D. Pa. Feb. 13, 2017). In a notice of supplemental authority, Plaintiffs also cite *In re Arby's Restaurant Group Inc. Litigation,* 17-cv-0514-AT, 2018 WL 2128441, at *7-8 (N.D. Ga. Mar. 5, 2018), which follows *Home Depot* and *Wendy's* in permitting a negligence per se claim to survive a motion to dismiss. Defendant distinguishes Plaintiffs' cases because they do not apply the law of any states at issue. *See, e.g., Community Bank,* 887 F.3d at 819 (affirming district court's refusal to predict Illinois or Missouri would allow negligence per se claim, *Home Depot* predicted the law of Georgia and "seems to have been incorrect"). Defendant also distinguishes *Home Depot* because it found Georgia law would permit the negligence per se claim in part based on cases alleging violations of FTC franchise regulations that are not at issue here which Plaintiffs rely. *See Home Depot,* 2016 WL 2897520, at *4 n.66 (citing *inter alia Bans Pasta).*

Plaintiffs did not cite any cases applying Arizona, Colorado or Missouri law to find Section 5 supports a negligence per se claim. The court is persuaded that Section 5's prohibition of "unfair ... practices in or affecting commerce" is too general to consider it a statutory duty within the meaning of negligence per se for Arizona, Colorado and Missouri law.

However, Plaintiffs also argue "Defendant's brief overlooks the Plaintiffs' authorities in support of their negligence *per se* claim that describe Defendant's duties," Doc. 57 (Response) (citing Doc. 36 ¶¶ 71-74, 128). Defendant did not reply to this point. The authorities Plaintiffs allege in the cited paragraphs of the Amended Complaint are the FTC's 2007 "published guidelines

that establish reasonable data security practices for businesses;" a 2011 guidance document entitled *Protecting Personal Information: A Guide for Business* (FTC Nov. 2011)[20], available from https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; and "orders against businesses that failed to employ reasonable measures to secure Payment Card Data." Doc. 36 ¶¶ 72-74.

A generic allegation of FTC orders, without providing any citations or quotes of specific conduct the FTC prohibited or required, is meaningless. Plaintiffs' allegations regarding the FTC's 2007 guidelines indicate it defines standards and practices that are more specific than Section 5's generic prohibition of "unfair practices," but Plaintiffs do not allege the 2007 guidelines state that failing to implement the "recommended" practices would violate Section 5. Doc. 36 ¶ 72. The same is true of Plaintiffs' allegations regarding the 2011 guidelines. *Id.* ¶ 73. Nor have Plaintiffs cited any authority that Arizona, Colorado or Missouri would recognize an agency's "guidance" as a statutory or regulatory duty that could support a negligence per se claim. Even if Plaintiffs had cited FTC orders or regulations referring to the data security practices from its guidelines, the Eleventh Circuit recently found the FTC cannot simply refer to a failure to employ "reasonable" data security measures to support an enforcement order under Section 5. *LabMD, Inc. v. Fed. Trade Comm'n,* No. 16-16270, 2018 WL 3056794, at *10 (11th Cir. June 6, 2018). The case does not address negligence per se but involved a similar standard of specificity. Under Rule 65, injunctive orders must "state the reasons for its coercive provisions, state the provisions 'specifically,' and describe the acts restrained or required 'in reasonable detail.'" *Id.* The court vacated the FTC's cease and desist order because it

> contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-

[20] The court has not reviewed the 2011 guidelines; the URL in the Amended Complaint is out of date and the FTC's website has only a 2016 edition, not the 2011.

> security program to meet an indeterminable standard of reasonableness. This command is unenforceable.

Id. at *11.

Given that the cases on which Plaintiffs rely for this claim do not apply Arizona, Colorado or Missouri law, the generality of Section 5 does not define a standard of conduct sufficiently specific to satisfy the elements of the claim in those states, and Plaintiffs' lack of citation to any FTC regulation or other official pronouncements in which the FTC prohibits specific conduct as a violation of Section 5, the court concludes the negligence per se claim fails. The court recommends dismissing Count 2.

3. Colorado Consumer Protection Act (Count 3)

Defendant moves to dismiss the Colorado Consumer Protection Act ("CCPA") claim because none of the named Plaintiffs live in Colorado and their transactions with Chipotle during the data breach occurred in each named Plaintiff's home state.

> Absent language in the statute evidencing a contrary intent, Colorado courts presume that a statute[ ] does not have extraterritorial effect. ... The presumption against extraterritorial effect can be overcome if a party presents authority manifesting a contrary intent from the Colorado legislature. ... The CCPA does not contain express language that it applies extraterritorially; accordingly, plaintiffs must overcome the presumption against extraterritorial application.

Airquip, Inc. v. HomeAdvisor, Inc., No. 16-cv-01849-PAB-KLM, 2017 WL 4222618, at *6 (D. Colo. Sept. 21, 2017) (internal quotation marks omitted, citing *Friedman v. Dollar Thrifty Auto. Grp., Inc.*, No. 12–cv–02432–WYD–KMT, 2013 WL 5448078, at *6 (D. Colo. Sept. 27, 2013); *Frontier Airlines, Inc. v. Dep't of Revenue*, 571 P.2d 1088, 1089 (Colo. 1977)).

In their response, Plaintiffs do not attempt to rebut the presumption against extraterritorial application. They first argue many unnamed class members are residents of Colorado. Defendant replies this is insufficient because named plaintiffs cannot rely on class members to state a claim, citing *Spokeo* 136 S. Ct. at 1547 n.6. *Spokeo* held that in order to establish injury for purposes of

standing, named plaintiffs in a purported class action cannot rely solely on the injuries of unnamed class members. The Tenth Circuit holds the same is true for purposes of stating a claim. "A putative class action complaint should be dismissed if the named plaintiff's individual claims fail to state a claim for relief." *Parrish v. Arvest Bank,* 717 F. App'x 756, 760 (10th Cir. 2017) (citing *Robey v. Shapiro, Marianos & Cejda, L.L.C.*, 434 F.3d 1208, 1213 (10th Cir. 2006)). The named plaintiffs must be able to state the CCPA claim themselves; they cannot rely on unnamed class members who may reside or were injured in Colorado.

Plaintiffs argue that it is enough for purposes of the CCPA that Chipotle engaged in much of its misconduct in Colorado, citing cases applying Minnesota and California law in support. In *Airquip*, the defendant allegedly engaged in its deceptive conduct at its headquarters in Colorado. The court focused on the locus of injury to the plaintiffs and dismissed the claim. "One of the requirements of a CCPA claim is that the challenged practice must significantly impact the public as actual or potential consumers of the defendant's goods, services, or property." *MDM Grp. Assocs., Inc. v. ResortQuest Int'l, Inc.,* No. 06-cv-01518-PSF-KLM, 2007 WL 2909408, at *8 (D. Colo. Oct. 1, 2007) (citing *inter alia Hall v. Walter,* 969 P.2d 224 (Colo. 1998)). In *MDM*, the defendant was alleged to have used the plaintiff's copyrighted brochure without a license in "several" states, apparently without specifying whether Colorado was among them. Based on the fact allegations, the court found "[t]here is no way to determine at this point the number of Colorado consumers who have been or may be affected by ResortQuest's challenged actions." *Id.* The court accordingly declined to dismiss the claim.

Here, however, none of the named Plaintiffs allege any facts suggesting Chipotle's alleged misconduct has affected them as actual or potential consumers in Colorado. None of the named

Plaintiffs made purchases from Chipotle in Colorado or allege they have suffered any harm in Colorado. The court recommends dismissing Count 3.

4. Implied Contract (Count 4)

As noted above, Plaintiffs allege they had an implied in fact contract with Chipotle, for Chipotle to use reasonable measures to secure the Plaintiffs' PII obtained in purchase transactions. Plaintiffs allege this contract based on the parties' use of the payment card systems to complete their transaction. They further point to Defendant's online privacy policy as an implied promise to follow that policy in its in-store transactions as well.

Defendant argues that under the law of all five states at issue, an implied in fact contract requires alleging an "offer, acceptance and consideration … albeit shown through conduct instead of words." Doc. 43 (motion) at 19 (citing *inter alia Virostek v. IndyMac Mortg. Servs.*, 2011 WL 6937185, at *10 (D. Colo. Sept. 6, 2011). Defendant argues Plaintiffs fail to allege conduct reflecting an offer and assent regarding data security services, viewing their transactions instead as solely agreements to purchase and sell food. Plaintiffs appear to agree regarding the elements of the claim, citing *Agritrack, Inc. v. DeJohn Housemoving, Inc.*, 25 P.3d, 1187, 1192 (Colo. 2001). Plaintiffs argue the existence of the implied contract is generally a question of fact for the jury, citing *Marsh v. Delta Air Lines, Inc.*, 952 F. Supp. 1458, 1466 (D. Colo. 1997).

Much as in *Engl*, 2016 WL 8578096, at *10-11 (D. Colo. June 20, 2016), Plaintiffs state enough facts to plausibly allege the elements for an implied contract regarding the security of their PII that Chipotle obtained in their transactions. Defendant cites cases holding that a transaction does not imply an agreement regarding data security in or after that transaction, arguing that data security is not necessary to purchase or sell a burrito using a payment card. But the alleged implied contract regards the means of payment (and security of the PII involved therein), not the purchase of goods. Does Chipotle's offer to accept payment cards as a means of payment imply that

Chipotle would take reasonable measures (or perhaps in other allegations in the Amended Complaint, the measures stated in its online privacy policy or the PCI contracts) to ensure the PII involved in a payment card transaction remains secure? Both sides cite cases from other circuits on this issue, but on the allegations Plaintiffs present here, it is a factual issue that cannot be resolved on the present motion. The court recommends denying the motion with respect to Count 4.

5. Unjust Enrichment (Count 5)

Plaintiffs allege Defendant is unjustly enriched, either by the entire amounts of Plaintiffs' purchases or by the portion thereof that should have been spent on reasonable data security measures for their PII. As noted above, in their argument regarding Ms. Baker and Mr. Lawson's standing, Plaintiffs disclaimed having brought an "overpayment" claim.

Defendant assumes that the "overpayment" prong is the only theory of this claim. In their response, Plaintiffs note they also allege unjust enrichment in the entire amount of their purchases. They allege they would not have made those purchases had Defendant disclosed that it was not taking reasonable data security measures to safeguard their PII. Plaintiffs cite in particular *In re Target*, 66 F. Supp. 3d at 1178 for this type of claim surviving Rule 12. In reply, Defendant distinguishes *Target* because the defendant in that case allegedly knew of the data breach while it was in progress and neither stopped it nor informed customers who shopped at its stores during the breach. Based on Defendant's assumption that Plaintiffs did not bring a "would not have shopped" type of claim, it argues *Target* is irrelevant.

On the one hand, since Defendant is the movant and bears the burden of showing it is entitled to dismissal of the claim, but does not actually address Plaintiffs' "would not have shopped" theory, the court could simply recommend denying the motion as to this part of Count V. But upon receiving such a recommendation, Defendant would no doubt find its reply regarding

Target to support a more expansive argument in objections. The court therefore will briefly address whether Plaintiffs' "would not have shopped" theory of unjust enrichment states a claim for relief.[21]

Under Colorado law, unjust enrichment claims require: "(1) [T]he defendant received a benefit (2) at the plaintiff's expense (3) under circumstances that would make it unjust for the defendant to retain the benefit without commensurate compensation." *City of Arvada ex rel. Arvada Police Dep't v. Denver Health & Hosp. Auth.*, 403 P.3d 609, 616 (Colo. 2017) (quoting *DCB Constr. Co., Inc. v. Central City Dev. Co.*, 965 P.2d 115, 119 (Colo. 1998)). "[I]njustice in this context requires some type of improper, deceitful, or misleading conduct" by the defendant. *DCB Construction*, 965 P.2d at 122.

Plaintiffs allege Chipotle received the benefit of the monies Plaintiffs paid in transactions they would not have engaged in, had they known it was not providing reasonable data security measures for those transactions. They allege Chipotle knew it was not providing reasonable data security because for instance it decided to not implement EMV technology despite the PCI requirement to do so in order to protect against the threat of malware in vendors' POS systems. Whether Plaintiffs in the end can prove these fact allegations show "improper, deceitful, or misleading conduct" for the third element of the claim is an open question, but the allegations suffice to plausibly allege unjust enrichment. The court therefore recommends denying the motion in part as to Count 5's allegation that Plaintiffs would not have made purchases from Chipotle, had

[21] At least for purposes of the present motion, the elements for this claim are the same in all five states. *See, e.g., City of Arvada ex rel. Arvada Police Dep't v. Denver Health & Hosp. Auth.*, 403 P.3d 609, 616 (Colo. 2017); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1071 (C.D. Ill. 2016) (Arizona and Illinois); *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762-63 (9th Cir. 2015) (California); *Hargis v. JLB Corp.*, 357 S.W.3d 574, 586 (Mo. 2011).

it disclosed it was not using reasonable data security measures and granting the motion in part as to Count 5's overpayment theory.

6. Arizona Consumer Fraud Act Claim (Count 6).

Mr. Gordon alleges Defendant's failure to disclose that its security systems were lacking is an actionable omission under the Arizona Consumer Fraud Act. ("ACFA").[22] Plaintiffs are silent regarding the manner in which Defendant should have made that disclosure. They do not point to a specific representation or statement (such as Chipotle's privacy policy) in which Defendant omitted this fact, which Mr. Gordon saw and relied upon. They appear to argue Defendant should have disclosed this fact in some fashion during its transaction with Mr. Gordon, *i.e.*, somewhere or somehow in its stores to alert Mr. Gordon to the company's allegedly inadequate data security before he used his payment card in the transaction. Doc. 57 at 18-19 (citing *inter alia State ex rel. Horne, v. Autozone, Inc.*, 275 P.3d 1278, 1281 (Ariz. 2012)).

Defendant argues even if the claim regards an omission, it still requires plaintiff to allege a statement or representation in which Chipotle should have disclosed the shortcomings of its security systems for customer PII. Doc. 64 (Reply) at 11-12. Defendant cites *In re Ariz. Theranos, Inc. Litig.*, 256 F. Supp. 3d 1009, 1028 (D. Ariz. 2017). The case does not support Defendant's contention; the holding therein that a statutory consumer fraud claim alleging an omission requires plaintiff to allege "where the omitted information should or could have been revealed" regards California law, not Arizona. *Id.* (quoting *Marolda v. Symantec Corp.*, 672 F.Supp.2d 992, 1002 (N.D. Cal. 2009)). Nor do any of Defendant's other cited cases support such a requirement for the ACFA. One of Plaintiffs' cited cases regards a merchant's failure to display prices "on

[22] The claim as pled actually refers to a wider variety of theories under the ACFA (doc. 36 ¶ 176), but Plaintiffs' response states that Mr. Gordon primarily focuses on an omission and makes little attempt to defend the claim on the other alleged theories.

merchandise or at the point of display" pursuant to another statute which required that display. *Autozone,* 275 P.3d at 1279. The court did not require plaintiff (the attorney general) to show an omission at the merchandise display rack was within the meaning of "omission" for purposes of the ACFA. Indeed, if alleging a separate, written statement or document was required, this would preclude a vast majority of merchant-consumer transactions from the ACFA, contrary to the statute's purpose of protecting consumers. See *Arizona Theranos,* 256 F. Supp. 3d 1009, 1022-23 (quoting *State ex rel. Woods v. Hameroff,* 180 Ariz. 380, 884 P.2d 266, 268 (1994)). Defendant does not show Mr. Gordon's ACFA claim fails as a matter of law, and the court recommends denying the motion as to Count 6.

7. California Customer Records Act, Cal. Civ. Code § 1798.80, et seq. (Count VII).

According to Defendant:

> The California plaintiffs allege that Chipotle violated two provisions of the California Customer Records Act: (1) failing to "implement and maintain reasonable security procedures and practices" under Cal. Civ. Code § 1798.81.5(b), and (2) failing to promptly notify them in violation of Cal. Civ. Code § 1798.82. But to state claim under the act, a customer must have suffered damages. Cal. Civ. Code § 1798.84(b).

Doc. 43 (Motion) at 23. Plaintiffs do not dispute this characterization of the claim and note the claim can stand on either or both Sections 1798.81.5(b) and 1798.82, citing *Boorstein v. CBS Interactive, Inc.,* 165 Cal. Rptr. 3d 669, 680 (Cal. App. 2013).

Defendant argues the claim fails because Plaintiffs cannot allege damages in merely their time and effort spent addressing fraudulent charges or the time and costs of monitoring for future identity theft. Section 1798.84(b) permits suit by "[a]ny customer injured by a violation of [the CRA]." Cal. Civ. Code § 1798.84(b). This statute clearly requires Plaintiffs to allege an injury from the Defendant's alleged violation of Sections 1798.81.5 and 1798.82; violations of the statute do not in themselves suffice to bring a private right of action. *Boorstein,* 165 Cal. Rptr. 3d at 680.

Defendant cites *Dugas v. Starwood Hotels & Resorts Worldwide*, 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, (S.D. Cal. Nov. 3, 2016). *Dugas* dismissed a Section 1798.82 delayed notice claim for lack of allegations to plausibly suggest the defendant's delay in notice caused any incremental harm. *Id.* at *7. But the court found plaintiff's alleged time spent and productivity lost in addressing the theft of his payment card information sufficed for both Article III standing and to state a claim under Section 1798.84 for the defendant's violation of Section 1798.81.5. *See also In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1218 (N.D. Cal. 2014) ("Although Section 1798.84 does not define what qualifies as an injury under the statute, other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact standard suffices to establish statutory injury under the CRA."); *Dieffenbach*, 887 F.3d at 829 (non-trivial amounts of time and money spent addressing violation of CRA satisfy the injury element of Section 1798.84).

Defendant cites several cases that find time and effort are not actionable damages, but those cases do not address a claim under the CRA. *See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 497 (Me. 2010). Here, the California named Plaintiffs each sufficiently allege time or money spent addressing the fraudulent charges and monitoring for future identity theft, and therefore plausibly allege injury from Defendant's alleged violation of Section 1798.81.5.

Here, Ms. Baker alleges in relevant part that

> [o]n April 3, 2017, three unauthorized charges were attempted on Plaintiff's debit card. She learned about the attempts via email alerts from her bank, for online purchases of $69.99, $19.99, and $49.99, respectively. The charge of $49.99 went through, but the others were declined.

Doc. 36 ¶ 14. Ms. Baker does not expressly allege what day she received the email alerts from her bank, but in order to plausibly allege harm from Chipotle delaying its announcement from April

25 to May 29, 2017, Ms. Baker would need to allege she did not learn of the charges until after April 25. Three weeks' delay in receiving bank email alerts would not be plausible.

Ms. Conard alleges that

> [o]n or about April 22, 2017, Plaintiff Conard received a call from her bank seeking approval for a $1,300 charge from Barcelona, Spain. Determining that Plaintiff Conard's credit card had been compromised, her bank closed the card account and re-issued a new credit card.

Doc. 36 ¶ 18. Ms. Conard thus learned of and took action regarding the fraudulent charges a few days before Chipotle learned of the data breach. She does not plausibly allege harm from Chipotle's delay in notice.

In contrast, the Mercers argue that they

> received a letter from their bank on June 15, 2017 stating that their debit card may have been exposed in the Chipotle Data Breach, more than 2 months after Chipotle learned of the Data Breach. *Id.* Plaintiffs allege that, had they been notified of the breach timely, they could have addressed the Breach earlier, and taken steps to prevent the fraud they experienced.

Doc. 57 (Response) at 22. See Doc. 36 ¶¶ 12-13. These facts plausibly suggest the Mercers could have begun to address the potential for their payment card to be used fraudulently, and perhaps could have avoided the fraudulent charges. Giving reasonable inferences, the Mercers could have stopped or changed automatic orders to prevent them from being cancelled or delayed. Doc. 36 ¶ 13. Therefore, the court recommends granting the motion in part as to Count 7, to dismiss only the part of the claim alleging a violation of Section 1798.82 brought by Ms. Baker and Ms. Conard.

8. California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. (Count 8)

To state a claim under the California Unfair Competition Law, Plaintiffs must allege they "suffered injuries in fact and . . . lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. "In order to establish standing under the UCL, a plaintiff's claim must specifically involve lost money or property." *Dugas,* 2016 WL 6523428, at *11 (citing *inter*

alia Kwikset Corp. v. Superior Court, 246 P.3d 877, 886 (Cal. 2011)). Plaintiffs argue they satisfy this element by alleging Defendant's failure to disclose its inadequate data security "deceived Plaintiffs into spending money to purchase products ... [that] but for Defendant's deception, Plaintiffs would not have made those purchases or would not have paid the amount they paid." Doc. 57 (Response) at 23 (citing *In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016)).[23] The court has already recommended dismissing the claims that allege overpayment, in part because Plaintiffs argued they did not bring such a claim for purposes of standing and in part because they do not plausibly allege that a portion of the purchase price was implicitly for data security measures. *See supra.*

Other data breach cases, such as *In re Sony* have allowed UCL claims to survive on the theory of overpayment that Plaintiffs argue here. However, those cases do not appear to involve transactions like those at issue here, in which the Defendant has a significant amount of cash customers for the same type of purchases. *In re Sony,* for instance, involved online transactions that *required* a payment card as the means of payment. 996 F. Supp. 2d at 954. As such, the absence of allegations that cash customers paid lower prices than Plaintiffs. Accordingly, for the same reasons the court recommends dismissing the "overpayment" theories with regard to standing and unjust enrichment, the court also recommends dismissing that portion of the UCL claim.

As for the remainder of the claim – that Plaintiffs would not have purchased from Chipotle at all had it disclosed the lack of reasonable data security – Defendant argues "[t]he types of damages that the California plaintiffs pleaded—unauthorized but reimbursed charges and time and effort responding to such charges—do not constitute lost money or property under California law." Defendant cites *Dugas,* 2016 WL 6523428, at *11; *Sony*, 903 F. Supp. 2d at 966; and *Kwikset*

[23] Plaintiffs argue that one of them alleges lost credit card points, but this was Mr. Lawson, a resident of Missouri. Plaintiffs do not explain why the California statute would apply to him.

Corp. v. Superior Court, 246 P.3d 877, 886 (Cal. 2011). Plaintiffs disagree, citing *Animal Legal Defense Fund v. LT Napa Partners LLC*, 234 Cal. App. 4th 1270, 1280-82 (2015), *review denied*, No. S225790 (Cal. June 10, 2015). *Animal Legal Defense Fund* found a "diversion of resources" in terms of time and effort spent "in response to, and to counteract, the effects of the defendants' alleged [misconduct] rather than in anticipation of litigation" sufficient for the "UCL's causation requirement for standing." *Id.* at 1284-85.

The court finds the reasoning in the 2014 *Sony* opinion persuasive. There plaintiffs alleged that had they known when they purchased game consoles from the defendant that it did not maintain reasonable data security for the online services those consoles were intended to play, they either would not have purchased them (or would have paid less). The court found these allegations sufficient to plausibly allege deprivation of money for purposes of the UCL. 996 F. Supp. 2d at 988.[24] Defendant's citation to the 2012 *Sony* opinion, *Dugas* and *Kwikset* are also not persuasive in light of *Animal Legal Defense Fund's* reasoning that *Kwikset's* citation to *Hall v. Time Inc.*, 158 Cal. App. 4th 847, 854-855, 70 Cal. Rptr. 3d 466, (Cal. App. 2008) impliedly recognizes time and effort spent redressing misconduct are sufficient injuries for the UCL. The court concludes Plaintiffs plausibly allege the loss of money in making purchases from Chipotle that they otherwise would not have made if it had disclosed it was not using reasonable data security measures.

Defendant next argues Plaintiffs do not allege reliance on any statement by Defendant, and in Defendant's view this is an element for the claim based on fraud. On this issue, Defendant cites cases applying that requirement to claims asserting misrepresentations, and it is unclear whether those cases include omissions as a form of misrepresentation. Plaintiff responds by citing *In re*

[24] Plaintiffs further argue that "damage to credit supports a UCL claim," citing *inter alia Izsak v. Wells Fargo Bank, N.A.*, No. C 13-05362 SI, 2014 WL 1478711, at *5 (N.D. Cal. Apr. 14, 2014). But none of the California Plaintiffs allege damage to credit. The Mercers allege an order was cancelled due to nonpayment but not any resulting damage to their credit.

Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1229 (N.D. Cal. 2014) and *Kwikset*, 51 Cal. 4th at 758, as support that their alleging they would not have made the purchases had they known the truth suffice to allege reliance under the UCL.

The "reliance" element of the UCL claim is also referred to as "a causal connection." *Kwikset*, 246 P.3d at 887. In this case, Plaintiffs do not allege a fraudulent misrepresentation for the UCL claim. They allege a failure to disclose. Doc. 36 ¶ 203. Misrepresentations and omissions are often analyzed separately under the UCL. *See, e.g., In re Sony*, 996 F. Supp. 3d at 991; *In re Adobe*, 66 F. Supp. 3d at 1229.[25] Defendant does not address what standard of causation applies for UCL claims based on fraudulent omissions. However, a case that Defendant cites with respect to another California statutory claim, *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033 (N.D. Cal. 2014), makes plain the same standard applies for both misrepresentations and omissions under the UCL: "a plaintiff must have actually relied on the misrepresentation or omission, and suffered economic injury as a result of that reliance, to have standing to sue." *Id.* at 1047-48 (citing *In re Tobacco II Cases*, 46 Cal. 4th 298, 326, 207 P.3d 20 (Cal. 2009)).

The court finds *Sony* and *Adobe* persuasive on this issue. Plaintiffs plausibly allege causation or reliance on Defendant's omission that it was not providing reasonable data security for its payment card transactions because that information is material to any reasonable consumer, and Plaintiffs allege they went ahead with payment card purchases that they would not have made had they known the truth. Doc. 36 ¶ 204. Defendant has not shown that the UCL's reliance element requires pleading anything further.

---

[25] In a footnote, Defendant argues it does not have a duty of disclose "outside the context of a threat to public safety," citing *Dana v. Hershey Co.*, 180 F. Supp. 3d 652, 665 (N.D. Cal. 2016). A single sentence in a footnote is insufficient to raise the issue. *Hill v. Kemp*, 478 F.3d 1236, 1255 n.21 (10th Cir. 2007). The court does not reach it.

Defendant further argues the "unfairness" portion of the claim fails because Plaintiffs' allegations do not entitle them to either form of remedy available for the UCL claim: restitution or injunction. Defendant cites *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1148-49 (2003). Defendant argues Plaintiffs do not allege facts to support that they are likely to suffer the same harm again (to support injunctive relief) and that Defendant "is not holding any funds belonging to plaintiffs" because their "overpayment" claim fails. In response, Plaintiffs argue they can show the same injury is likely to recur based on a pattern of officially sanctioned behavior that violates the statute. Plaintiffs cite *inter alia Armstrong v. Davis*, 275 F.3d 849, 861 (9th Cir. 2001). *Armstrong* addresses federal anti-discrimination claims, not UCL claims. However, in its reply, Defendant did not dispute that California would apply the same standards for injunctive relief under the UCL.

In the absence of Defendant citing any cases to support the UCL does not permit injunctive relief based on a pattern of officially sanctioned behavior, in light of Plaintiffs alleging Defendant experienced a significant data security breach in 2004 and nonetheless chose not to upgrade its POS system to keep pace with data security, if Plaintiffs prove their allegations they could be entitled to injunctive relief. It may be Plaintiffs will have difficulty proving that they would make payment card purchases again at Chipotle, but that appears to be a fact issue for the UCL claim. As for restitution, Defendant does not address Plaintiffs' theory that they are entitled to refunds of the entire purchase amounts. In short, the court recommends denying the motion to dismiss as to the "would not have purchased" theory in Count 8, and granting the motion to dismiss as to the "overpayment" theory therein.

9. California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") (Count 9)

Plaintiffs allege Defendant engaged in "deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "services" and "goods" (as defined in the CLRA)." Doc. 36 ¶ 214.

Defendant makes largely the same arguments regarding this claim as the UCL claim. Defendant first argues Plaintiffs must specifically plead they relied on Defendant's allegedly deceptive conduct, whether it be misrepresentations or omissions. In response, Plaintiffs appear to concede they do not allege an affirmative misrepresentation for this claim and instead rely on the same alleged omission as under the UCL: Defendant's failure to disclose that it did not provide reasonable data security measures for payment card transactions. Much as they allege for the UCL claim the California Plaintiffs allege for this claim that "Defendant intended that Plaintiff Baker, Plaintiff Conard, the Mercer Plaintiffs, and the Class rely on" its alleged deceptive and unfair practices, including its omission. Doc. 36 ¶ 216. Plaintiffs allege they suffered harm as a result of Defendant's failure to disclose – namely they went ahead the purchases, their PII was stolen, they incurred fraudulent charges, and had to spend more than de minimis time addressing the fraud and as to Ms. Conard, money to monitor for identity theft. The California Plaintiffs do not allege they relied on a specific misrepresentation, but they allege they would not have made purchases from Defendant had they known the non-disclosed facts.

Much as with the UCL claim, Defendant does not show the CLRA claim requires the California Plaintiffs to allege more facts to plausibly suggest they relied on Defendant's omission in making the purchases that they allege caused them to incur time (and as to Ms. Conard, also money) addressing fraud. Defendant relies on *Massachusetts Mut. Life Ins. Co. v. Superior Court*, 97 Cal. App. 4th 1282, 1291, 119 Cal. Rptr. 2d 190 (2002). But *Mass Mutual* held "[t]he rule in

this state and elsewhere is that it is not necessary to show reliance upon false representations by direct evidence. The fact of reliance upon alleged false representations may be inferred from the circumstances attending the transaction." 119 Cal. Rptr. at 197 (internal quotation marks omitted). In that case, the plaintiffs

> contend[ed] Mass Mutual failed to disclose its own concerns about the premiums it was paying and that those concerns would have been material to any reasonable person contemplating the purchase of an N-Pay premium payment plan. If plaintiffs are successful in proving these facts, the purchases common to each class member would in turn be sufficient to give rise to the inference of common reliance on representations which were materially deficient.

Id. at 198. "If the undisclosed [information] ... was material, an inference of reliance as to the entire class would arise, subject to any rebuttal evidence [the defendant] ... might offer." *Id.* at 199. Another of Defendant's cited cases, *In re Fluidmaster, Inc., Prods. Liab. Litig.*, 2017 U.S. Dist. LEXIS 48792, 2017 WL 1196990 (N.D. Ill. Mar. 31, 2017), makes the same point:

> An essential element for a fraudulent omission claim [under CLRA] is actual reliance. ... In fact, actual reliance must be established for an award of damages under the CLRA. * * * To prove reliance on an omission, a plaintiff must show that the defendant's nondisclosure was an immediate cause of the plaintiff's injury-producing conduct. ... The nondisclosure must be a "substantial factor" in the decision to purchase the product. Reliance can be "presumed, or at least inferred, when the omission is material, which is based on the objective reasonable consumer standard.

Fluidmaster, 2017 U.S. Dist. LEXIS 48792, at *163 (internal quotation marks and citations omitted, citing *Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015); *Cohen v. DIRECTV, Inc.*, 178 Cal. App. 4th 966, 980, 101 Cal. Rptr. 3d 37 (2009)).[26] *See also Stearns v. Ticketmaster Corp.*, 655 F.3d 1013, 1022 (9th Cir. 2011).

[26] In its reply, Defendant also cites *Mirkin v. Wasserman*, 5 Cal. 4th 1082, 1093 (1993), arguing to state an omission-based claim under the CLRA a plaintiff must plead that "had the omitted information been disclosed, *one would have been aware of it* and behaved differently." *Daniel* finds *Mirkin* persuasive for a CLRA claim, but the case does not appear to address the CLRA. Either way, Plaintiffs allege they would have been aware if Chipotle had posted or otherwise told them the nondisclosed information in their transactions and would not have made the purchases.

Defendant relies on *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1049 (N.D. Cal. 2014), a case in which the plaintiffs alleged they would not have purchased iPhones or would not have paid as much, if Apple had disclosed that they would be unable to use messaging services if they thereafter switched to non-Apple smartphones. The court noted plaintiffs did not expressly allege they relied on Apple's misrepresentation or omission when they made their purchases, did not allege Apple knew the solution it proposed at the time was ineffective when plaintiffs made those purchases, and plaintiffs alleged this iPhone problem was known to others (it was a subject of a CNET News article). *Id.* at 1049. In light of those unique facts, the court concluded the plaintiffs failed to plausibly allege reliance on the defendant's omission. But the same is not true here; Plaintiffs allege Defendant knew it was not using reasonable data security measures when it accepted Plaintiffs' payment cards for their purchases. They allege this was not publicly known at the time.[27] In short, Defendant does not show the CLRA claim fails for lack of plausible reliance on its alleged omission. *See also In re Sony,* 996 F. Supp. 2d at 992.

Defendant next argues the CLRA claim requires damages that the California named Plaintiffs do not allege. Defendant cites *Brazil v. Dell Inc.*, 585 F. Supp. 2d 1158, 1164 (N.D. Cal. 2008), which held ""plaintiffs in a CLRA action [must] show not only that a defendant's conduct was deceptive but that the deception caused them harm." Defendant believes that "pure time and effort" are not actual damages for purposes of the CLRA. Even if this were a correct statement of the law, Defendant ignores the money Ms. Conard alleges she spends for LifeLock credit monitoring as a result of Defendant's alleged conduct. Doc. 36 ¶ 18.

---

[27] Defendant also cites *Annunziato v. eMachines, Inc.*, 402 F. Supp. 2d 1133, 1136 (C.D. Cal. 2005); while the case notes the CLRA has a reliance or causation requirement, it does not address what the element requires.

Plaintiffs argue the CLRA just requires the consumer to suffer "any damage" from any "method, act, or practice" made unlawful by the Act. Cal. Civ. Code §§ 1780(a), 1781(a). Plaintiffs argue "any damage" includes pecuniary and non-pecuniary damages alike, including transaction costs and opportunity costs, citing *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 640, 643, 200 P.3d 295 (Cal. 2009). Defendants did not attempt to rebut this case. Plaintiffs' allegations of time and effort (and in Ms. Conard's instance, money spent) addressing the fraud they allege resulted from Defendant's conduct plausibly allege actionable damages under the CLRA. Accordingly, the court recommends denying the motion with respect to count 9.

10. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505/1, et seq. *("Illinois CFA") (Count 10)*

The Illinois CFA declares unlawful the "unfair or deceptive acts or practices, including … misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon [it] … in the conduct of trade or commerce… whether any person has in fact been misled, deceived or damaged thereby." 815 Ill. Comp. Stat. § 505/2. The private right of action is limited to "[a]ny person who suffers actual damage as a result of a violation of this Act." *Id.* § 505/10(a).

Defendant argues Ms. Fowler must allege she actually saw and was deceived by Defendant's statements, citing *Barbara's Sales, Inc. v. Intel Corp.*, 879 N.E.2d 910, 927 (Ill. 2007), which notes "plaintiffs must prove that each and every consumer who seeks redress actually saw and was deceived by the statements in question." Plaintiffs rely instead on *Cozzi Iron & Metal v. U.S. Office Equip.*, 250 F.3d 570, 576 (7th Cir. 2001). *Cozzi* held that the misrepresentation must regard information that is material to a buyer or essential to the transaction, but that Illinois state courts (at the time) did not require the plaintiff to show reliance for the claim. *Id.* But *Barbara's Sales* cites a case post-dating *Cozzi,* in which the Illinois state courts held for ICFA claims alleging

fraudulent misrepresentation "a plaintiff must prove that he or she was actually deceived by the misrepresentation in order to establish the element of proximate causation." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 861 (Ill. 2005).

However as noted already, Plaintiffs largely concede they do not allege a misrepresentation. They allege a deceptive omission. Defendant's briefs and cited cases do not make plain whether Illinois state courts apply the same standard of actual deception to ICFA omission claims. In this regard, Plaintiffs' case *Blankenship v. Pushpin Holdings*, No. 14 C 6636, 2015 U.S. Dist. LEXIS 135944, at *25-26 (N.D. Ill. Oct. 6, 2015), is on point. Plaintiffs plausibly allege reliance because they allege Defendant's failure to disclose (inferably, in its in-store transactions) that its system for payment cards was not reasonably secure is a material omission that if they had known, they would not have made the purchases. See Doc. 36 ¶¶ 230, 231 ("omission of material facts" alleged in several bullet points).

Defendant further argues as to both the fraudulent/deceptive and unfair practices prongs that Ms. Fowler alleges only time and effort addressing the fraudulent charges on her compromised card. Defendant argues these do not constitute actual damages within the meaning of the Illinois CFA. However, Defendant recognizes Ms. Fowler also alleges she suffered further identity theft in the form of unauthorized accounts being opened in her name. Defendant argues it did not cause that harm because the data breach did not involve any of the PII that is necessary to enable such identity theft. Doc. 43 (Motion) at 28. But the court concluded above that in this case, there is a fact issue whether the data breach involved more PII than payment card information. Defendant is free to pursue this issue in discovery, but the court cannot resolve it on a motion to dismiss. The court declines to reach whether Ms. Fowler's time and effort spent addressing the unauthorized

use of her payment card is sufficient in itself for the damages element. The court recommends denying the motion on Count 10.

11. Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. §§ 510/1, et seq. ("Illinois DTPA") (Count 11)

[T]he IUDTPA ... is primarily directed to unfair competition between businesses rather than consumer protection." *Darne v. Ford Motor Co.*, No. 13 C 03594, 2015 U.S. Dist. LEXIS 169752, at *41 (N.D. Ill. Dec. 18, 2015). Defendant argues this claim provides only injunctive relief and requires Ms. Fowler to allege she is at risk of future harm from Defendant's deceptive trade practice, citing *ATC Healthcare Servs., Inc. v. RCM Techs., Inc.*, 282 F. Supp. 3d 1043 (N.D. Ill. 2017), and *Darne*, 2015 WL 9259455, at *12.

"The likelihood of future harm occurring absent an injunction is an element of liability on the claim, not merely a separate element of damages." *ATC Healthcare*, 282 F. Supp. 3d at 1050 (citing *Glazewski v. Coronet Ins. Co.*, 483 N.E.2d 1263, 1267 (Ill. 1985)). "Proving the likelihood of future harm is difficult under the IUDTPA because the harm from the allegedly deceptive practice has usually already occurred." *Darne*, 2015 U.S. Dist. LEXIS 169752, at *41. *ATC Healthcare* dismissed an Illinois DTPA claim that did not allege the defendant's misconduct (an "attempted takeover" of its employees) toward the plaintiff was ongoing or likely to recur. Defendant further argues that "[w]here, as here, the plaintiff becomes 'aware' of the challenged practice, she 'is not likely to be harmed in the future' by those practices," citing *Demecidis v. CVS Health Corp.*, 2017 WL 569157, at *2 (N.D. Ill. Feb. 13, 2017). *See also Darne*, 2015 U.S. Dist. LEXIS 169752, at *43 (even if risks of future losses on purchased vehicles came to fruition, plaintiff "cannot allege that it will be deceived in the future, so the ILDTPA is inappropriate to address the damages it alleges.").

Ms. Fowler argues she is at risk of future harm because "Defendant continues to utilize payment systems in the operation of its business," and given that its 2004 data breach experience did not lead Chipotle to maintain reasonable measures she cannot rely on its representations in the future, citing *Davidson v. Kimberly-Clark Corp.*, 873 F.3d 1103, 1116 (9th Cir. 2017). However, *Davidson* regards California statutory claims. Its reasoning is opposite to the Illinois courts' construction of the Illinois DTPA. *Id.* at 1107. Count 11 also does not allege Ms. Fowler is at risk of the same harm in the future. The court recommends dismissing Count 11.

12. Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), et seq. ("MMPA") (Count 12)

Defendant argues Mr. Lawson fails to allege "an ascertainable loss of money or property" from Defendant's alleged violation of the MMPA and therefore fails to state the claim. Defendant cites *Hess v. Chase Manhattan Bank, USA, N.A.*, 220 S.W.3d 758, 773 (Mo. 2007). Defendant notes Mr. Lawson alleges time and effort spent addressing the credit card fraud, and argues this is insufficient; Plaintiffs argue to the contrary. Defendant further argues Mr. Lawson's out of pocket expense (to expedite a new payment card) does not count either, because it was self-inflicted under *Engl.*

In its analysis above regarding Mr. Lawson's standing, the court concludes that Defendant is raising a fact issue regarding whether Mr. Lawson's out of pocket expense should be deemed a damage resulting from the data breach. That issue cannot be resolved on the present motion. The court declines to reach whether Mr. Lawson's time and effort would in themselves plausibly allege the damages element for this claim. The court recommends denying the motion as to Count 12.

III. CONCLUSION

For each of the reasons stated above, the court RECOMMENDS as follows:

- *Granting in part and denying in part* the motion to dismiss Plaintiffs Baker and Lawson for lack of standing, to dismiss only the allegations of independent value in Plaintiffs' stolen PII and overpayment;
- *Granting* the motion to dismiss Counts 1, 2, 3, and 11;
- *Denying* the motion to dismiss Counts 4, 6, 9, 10 and 12; and
- *Granting in part and denying in part* the motion to dismiss Counts 5, 7 and 8.

It does not appear that Plaintiffs sought leave to amend the Amended Complaint. The court nonetheless RECOMMENDS allowing Plaintiffs to file a motion to amend to the extent they can allege facts to cure the flaws noted.

ADVISEMENT TO THE PARTIES

Within fourteen days after entry of the Recommendation, any party may file objections to the Magistrate Judge' s proposed findings and recommendations. 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b); *In re Griego*, 64 F.3d 580, 583 (10th Cir. 1995). A general objection that does not put the district court on notice of the basis for the objection will not preserve the objection for *de novo* review. " [A] party' s objections to the magistrate judge' s report and recommendation must be both timely and specific to preserve an issue for *de novo* review." *United States v. One Parcel of Real Prop. Known As 2121 East 30th Street, Tulsa, Okla.*, 73 F.3d 1057, 1060 (10th Cir. 1996). Failure to make timely objections may bar de novo review by the district court and will result in waiver of the right to appeal from a judgment of the district court based on the recommendation. *See Vega v. Suthers*, 195 F.3d 573, 579-80 (10th Cir. 1999) (a district court' s decision to review a magistrate judge' s recommendation de novo despite the lack of an objection does not preclude

application of the "firm waiver rule"); *One Parcel of Real Prop.*, 73 F.3d at 1059-60 (objections to the magistrate judge' s recommendation must be both timely and specific to preserve the issue for *de novo* review by the district court or appellate review); *Int'l Surplus Lines Ins. Co. v. Wyo. Coal Ref. Sys., Inc.*, 52 F.3d 901, 904 (10th Cir. 1995) (by failing to object to certain portions of the magistrate judge' s order, cross-claimant waived its right to appeal those portions of the ruling); *Ayala v. United States*, 980 F.2d 1342, 1352 (10th Cir. 1992) (by failing to file objections, plaintiffs waived their right to appeal the magistrate judge's ruling); *but see, Morales-Fernandez v. INS*, 418 F.3d 1116, 1122 (10th Cir. 2005) (firm waiver rule does not apply when the interests of justice require review).

DATED this 1st day of August 2018.

BY THE COURT:

Mark L. Carman
United States Magistrate Judge