IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

	:	
	:	1:20-cv-382
IN RE RUTTER'S INC. DATA SECURITY BREACH LITIGATION	:	
	:	Hon. John E. Jones III
	:	

MEMORANDUM AND ORDER

January 5, 2021

The matter presently before the Court is a putative class action arising out of a data breach by third-party cybercriminals. Plaintiffs are four Pennsylvanians who used their credit or debit cards to make purchases at various Rutter's convenience stores and gas stations. They each filed suit against Rutter's after the company reported that payment card data had potentially been improperly accessed over an eight- or nine-month period from late summer 2018 through May 2019 (the "Breach Period"). The four actions were consolidated, and Rutter's has now moved to dismiss all claims. For the following reasons, we will grant in part and deny in part the motion to dismiss.

I. BACKGROUND

In accordance with the standard of review applicable to a motion to dismiss, the following facts are derived from the operative complaint and viewed in the light most favorable to the Plaintiffs.

Defendant CHR Corporation, d/b/a Rutter's ("Rutter's") is a Pennsylvania corporation that operates 72 convenience stores in Central Pennsylvania. (Doc. 30 at ¶ 26). Many of these stores also operate as gas stations. (*Id.*).

On February 13, 2020, Rutter's posted a statement to its website announcing the results of a third-party investigation into a possible data breach. (*Id.* at ¶ 31). According to that announcement, "the investigation identified evidence indicating that an unauthorized actor may have accessed payment card data from cards used on point-of-sale (POS) devices at some fuel pumps and inside some of our convenience stores through malware installed on the payment processing systems." (*Id.*). Rutter's said that "specific timeframes when data from cards used at the locations involved may have been accessed vary by location over the general timeframe beginning October 1, 2018 through May 29, 2019." (*Id.*). One Rutter's location, however, may have been implicated by the malware starting August 30, 2018, while nine other stores may have been affected as early as September 20. (*Id.*). The malware targeted information including customers' names, credit or debit card numbers, expiration dates, and internal verification codes, but for

customers who paid at POS devices that accept EMV-capable cards (Europay, MasterCard, and Visa), it was believed that the malware only collected the numbers and expiration dates of those cards. (*Id.* at ¶ 33). Plaintiffs aver that, according to security experts, thieves can still make fraudulent purchases even without a card's three-digit security code. (*Id.* at ¶ 37).

In response to the breach, Rutter's advised its customers to review their payment card statements for unauthorized activity and to utilize free credit reporting services. (*Id.* at ¶¶ 34–35). Plaintiffs allege this response did not "provid[e] meaningful assistance to consumers . . . . [i]n contrast to what is and has been frequently made available to consumers in recent data breaches," such as "monitoring services or fraud insurance[.]" (*Id.* at ¶ 36).

In all, Plaintiffs allege that Rutter's "failed to properly safeguard [putative] class members' Card Information" despite a "continuing duty pursuant to common law, industry standards, card network rules, and representations made in its own privacy policy to keep consumers' Card Information confidential and to protect it from unauthorized access." (*Id.* at ¶¶ 38–39). According to Plaintiffs, Rutter's had also been on notice from a "Security Alert" issued by Visa in November 2019 that warned of "criminal threat actors" increasingly targeting POS systems at "fuel dispenser merchants" due to the "slower migration to chip technology on many terminals[.]" (*Id.* at ¶ 41). Because many fuel dispensing merchants still utilize

"magnetic stripe payment card" systems instead of chip readers, Visa said such merchants were "an attractive target" for hackers. (*Id.*). Visa warned that "[f]uel dispenser merchants should take note of this activity" and that "these attacks have the potential to compromise a high volume of payment accounts." (*Id.*). Plaintiffs allege that "Rutter's failed to improve its cardholder data security despite these known critical risks." (*Id.* at ¶ 43). Specifically, Plaintiffs list six different examples of data security failures by Rutter's, including inadequate safeguarding of card information, inadequate maintenance of its data security environment to reduce the risk of a data breach, improper monitoring of its data security systems for existing intrusions and weaknesses, a failure to perform "penetration tests to determine the strength of its payment card processing systems," improper training of its information technology staff, and its failure to "retain outside vendors to periodically test its payment card processing systems." (*Id.* at ¶ 48).

Plaintiffs also point to the Payment Card Industry Data Security Standards ("PCI DSS"), promulgated by the Payment Card Industry Security Standards Council, which "apply to all organizations that store, process or transmit card data." (*Id.* at ¶ 50). Among these "detailed comprehensive requirements" is a "mandate" to "protect all systems against malware," and a requirement to "[t]rack and monitor all access to network resources." (*Id.* at ¶¶ 51–53). Plaintiffs allege that Rutter's violated these standards as well as "numerous other provisions of the

PCI DDS." (*Id.* at ¶ 54). According to Plaintiffs, "[i]ndustry experts acknowledge that a data breach is indicative of data security failures." (*Id.* at ¶ 57). Plaintiffs also allege that Rutter's violated the Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, through its "failure to employ reasonable measures to protect against unauthorized access to confidential consumer data." (*Id.* at ¶¶ 58–62).

The first action against Rutter's arising out of this data breach was filed by Plaintiff Lloyd Collins on March 4, 2020. (Doc. 1). Two days later, Plaintiff Morgan K. Palermo filed her own suit against Rutter's. *Palermo v. Rutter's Holdings, Inc. et al*., No. 1:20-cv-398 (M.D. Pa. March 6, 2020). On March 26, 2020, we issued an order consolidating the *Collins* and *Palermo* actions as well as any future actions relating to the data breach. (Doc. 12). On April 3, 2020, we issued a second order adding two subsequently-filed suits—one filed by Plaintiff Kathleen Johnson and one by Plaintiff Jon Lavezza—into the consolidated action. (Doc. 17). Plaintiffs collectively filed the operative Amended Complaint on May 22, 2020. (Doc. 30).

The Amended Complaint brings forth five causes of action against Rutter's: negligence (Count I); negligence per se (Count II); breach of implied contract (Count III); violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL") (Count IV); and unjust enrichment (Count V). (*Id.* at

¶¶ 90–150). Plaintiffs seek class certification; an award of compensatory, consequential, statutory, and treble damages; injunctive relief compelling Rutter's to strengthen its data security and monitoring systems, submit to future audits of those systems, and provide class members with "several years" of free credit monitoring and identity theft insurance; and an award of attorneys' fees, costs, and expenses, as well as pre- and post-judgment interest. (*Id.* at 43). Defendant Rutter's now seeks dismissal of the Amended Complaint in its entirety, and/or dismissal of Plaintiffs Johnson and Palermo for lack of standing. (Doc. 45) (the "Motion").

The Amended Complaint details the injuries allegedly incurred by each of the four plaintiffs in the data breach. Because Rutter's lodges a partial standing challenge, we will individually summarize Plaintiffs' injuries.

a. Lloyd F. Collins

Plaintiff Collins alleges that he used a Chase credit card at Rutter's Shippensburg location—one of the stores Rutter's identified as having been impacted by the breach—on September 2, September 15, September 20, October 1, October 5, and December 12, 2018. (Doc. 30 at ¶ 8). On February 24, 2020, Plaintiff Collins discovered on his credit card account a fraudulent purchase in the amount of $2,477 from United Airlines. (*Id.* at ¶ 9). Chase promptly notified him of the fraudulent activity, and, after Plaintiff Collins disputed the charge, Chase

cancelled the credit card and sent him a replacement, which took several days to arrive. (*Id.*). Chase also reimbursed Plaintiff Collins for the fraudulent charge, but it took three business days for those funds to appear in his account. (*Id.* at ¶ 10). Overall, Plaintiff Collins alleges he spent several hours engaging in remedial activity—in addition to his communications with Chase, Plaintiff Collins also updated various vendors with his new credit card information and set up fraud alerts for his credit history. (*Id.*). Plaintiff Collins avers that "[h]ad he known that Rutter's would not adequately protect his sensitive Card Information, he would not have made purchases at Rutter's." (*Id.* at ¶ 12).

b. Jon Lavezza

Plaintiff Lavezza alleges that he regularly made purchases at multiple Rutter's locations during the Breach Period. (*Id.* at ¶ 13). On around March 4, 2019, Plaintiff Lavezza discovered that his checking account (containing $1,854.96) was "compromised and emptied as a result of unauthorized access," which resulted in multiple overdraft fees. (*Id.* at ¶ 14). For "several days," he did not have access to his checking account, and it took one week for a new debit card to arrive. (*Id.* at ¶ 15). Like Plaintiff Collins, Plaintiff Lavezza alleges he lost "significant time" dealing with these troubles—he allegedly left work early one day, missed more work to file a police report, and missed another half day speaking to his bank—in addition to the "several gallons of gas" he expended

driving around town remedying his injuries. (*Id.* at ¶ 16). Like Plaintiff Collins, Plaintiff Lavezza would not have made purchases at Rutter's had he known his credit card information would not be adequately protected. (*Id.* at ¶ 18).

c. Kathleen Johnson

Unlike Plaintiffs Collins and Lavezza, Plaintiff Johnson does not allege that her credit or debit card information was ever compromised. Rutter's notified her via letter received on February 13, 2020, that its systems had been compromised during the Breach Period. (*Id.* at ¶ 19). Though none of her financial or personal information was (or has yet to be) improperly accessed or converted because of the data breach, Plaintiff Johnson nonetheless alleges a "continuing interest in ensuring that her Card Information is protected and safeguarded from future breaches." (*Id.* at ¶ 20). Accordingly, she now "review[s] her credit reports with greater frequency," but, although she says she "has lost time as a result of [Rutter's] data security failures," she does not specify how much lost time she has incurred. (*Id.* at ¶ 22). Plaintiff Johnson also avers that she would not have made purchases at Rutter's if she knew her credit card information would not have been protected. (*Id.* at ¶ 21).

d. Morgan K. Palermo

Plaintiff Palermo's injuries are more akin to those allegedly suffered by Plaintiff Johnson. She claims to have regularly made purchases at multiple Rutter's stores with her credit and/or debit card during the Breach Period, and,

therefore, her credit and/or debit card information was potentially compromised during the data breach. (*Id.* at ¶ 23). Like Plaintiff Johnson, Plaintiff Palermo has a "continuing interest in ensuring that her Card Information is protected and safeguarded from future breaches." (*Id.* at ¶ 24). And just as the other three Plaintiffs, she claims that she would not have made purchases at Rutter's if she knew her credit card information would not have been adequately protected. (*Id.* at ¶ 25).

II. STANDARD OF REVIEW

In considering a motion to dismiss pursuant to Rule 12(b)(6), courts "accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." *Phillips v. Cty. of Allegheny*, 515 F.3d 224, 231 (3d Cir. 2008) (quoting *Pinker v. Roche Holdings, Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002)). In resolving a motion to dismiss pursuant to Rule 12(b)(6), a court generally should consider only the allegations in the complaint, as well as "documents that are attached to or submitted with the complaint, . . . and any matters incorporated by reference or integral to the claim, items subject to judicial notice, matters of public record, orders, [and] items appearing in the record of the case." *Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006).

A Rule 12(b)(6) motion tests the sufficiency of the complaint against the pleading requirement of Rule 8(a). Rule 8(a)(2) requires that a complaint contain a short and plain statement of the claim showing that the pleader is entitled to relief, "in order to give the defendant fair notice of what the claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). While a complaint attacked by Rule 12(b)(6) motion to dismiss need not contain detailed factual allegations, it must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). To survive a motion to dismiss, a civil plaintiff must allege facts that "raise a right to relief above the speculative level…." *Victaulic Co. v. Tieman*, 499 F.3d 227, 235 (3d Cir. 2007) (quoting *Twombly*, 550 U.S. at 555). Accordingly, to satisfy the plausibility standard, the complaint must indicate that defendant's liability is more than "a sheer possibility." *Iqbal*, 556 U.S. at 678. "Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of entitlement to relief.'" *Id.* (quoting *Twombly*, 550 U.S. at 557).

Under the two-pronged approach articulated in *Twombly* and later formalized in *Iqbal*, a district court must first identify all factual allegations that constitute nothing more than "legal conclusions" or "naked assertions." *Twombly*,

550 U.S. at 555, 557. Such allegations are "not entitled to the assumption of truth" and must be disregarded for purposes of resolving a 12(b)(6) motion to dismiss. *Iqbal*, 556 U.S. at 679. Next, the district court must identify "the 'nub' of the … complaint – the well-pleaded, nonconclusory factual allegation[s]." *Id.* Taking these allegations as true, the district judge must then determine whether the complaint states a plausible claim for relief. *See id.*

However, "a complaint may not be dismissed merely because it appears unlikely that the plaintiff can prove those facts or will ultimately prevail on the merits." *Phillips*, 515 F.3d at 231 (citing *Twombly*, 550 U.S. at 556–57). Rule 8 "does not impose a probability requirement at the pleading stage, but instead simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element." *Id.* at 234.

III. DISCUSSION

Defendant Rutter's seeks dismissal of all five of Plaintiffs' claims, plus dismissal of Plaintiffs Johnson and Palermo for want of Article III standing. We will first consider the challenge to standing as to those two Plaintiffs, followed by an analysis of Plaintiffs' substantive claims. For the following reasons, we will dismiss from this action Plaintiffs Johnson and Palermo, as they fail to allege a concrete injury-in-fact, and we will dismiss Counts II and IV, but we will deny the remainder of the Motion.

A. Plaintiffs Johnson and Palermo Lack Standing

Article III of our Constitution limits our jurisdiction to actual "cases and controversies." U.S. CONST., art. III, § 2. For a plaintiff to establish Article III standing, the plaintiff must suffer an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). In other words, a "plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo, Inc. v. Robins*, 578 U.S. __, 136 S. Ct. 1540, 1548 (2016). To be "concrete," the plaintiff's injury "must be '*de facto*'; that is, it must actually exist." *Id.* Allegations of "possible future injury" are insufficient. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564 n.2 (1992).

Rutter's argues that the harms allegedly suffered by Plaintiffs Johnson and Palermo are insufficient to confer standing. In support, Rutter's principally relies on the Third Circuit's decision in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). *Reilly*, like the present action, involved a data security breach by an unknown cybercriminal. *Reilly*, 664 F.3d at 40. The *Reilly* hacker infiltrated defendant's payroll processing system and "potentially gained access to personal

and financial information" belonging to nearly 30,000 people, though the extent to which the hacker read, copied, or understood the data could not be ascertained. *Id.* The Third Circuit concluded that plaintiffs, who did not allege that they suffered any present injury, lacked standing. *Id.* at 42. Plaintiffs' allegations relied solely on conjecture: there was no allegation that their personal information had actually been compromised or misused, and, instead, they only alleged potential, future harm due to the breach. *Id.* The Third Circuit held that in "data breach cases where no misuse is alleged, . . . there has been no injury[.]" *Id.* at 45. "[I]ndeed," there is "no change in the status quo" in such a situation—the plaintiffs' credit card statements looked "exactly the same today as they would have been had [defendant's] database never been hacked." *Id.* And because any future injuries were "entirely speculative and dependent on the skill and intent of the hacker," there was no "quantifiable risk of damage in the future." *Id.* Finally, the Court concluded that allegations of lost time and money expenditures incurred by plaintiffs to monitor their financial information following a data breach are also insufficient to confer Article III standing "because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts" are not *actual injuries*. *Id*. at 46 ("That a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a 'concrete and particularized' or 'actual or imminent' injury.'").

We reached a similar conclusion in *Storm v. Paytime*, 90 F. Supp. 3d 359 (M.D. Pa. 2015). *Storm*, like both *Reilly* and this action, featured plaintiffs who alleged to have spent time and money (and for one plaintiff, certain travel expenses) protecting themselves from the risk of future identity theft following a third-party data breach of the defendant's payroll processing system. *Storm*, 90 F. Supp. 3d at 363. We concluded that the plaintiffs' alleged harms were insufficient to confer Article III standing, where plaintiffs had not alleged actual "misuse" of their information—as in *Reilly*, plaintiffs' credit card and bank accounts seemingly went untouched in the data breach. *Id.* at 366. Further, the allegation that plaintiffs were at an increased risk of identity theft was similarly insufficient; indeed, one year had passed since the data breach and no plaintiff was able to allege that they had become "actual victims of identity theft." *Id.* at 366–67. We opined that "[p]erhaps th[e] strict imminency standard has some wisdom," because even a "layperson with a common sense notion of 'imminency' would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future." *Id.* Even the plaintiff who incurred extra travel costs and related expenses did not have standing—those expenses, "although surely unfortunate, are merely a form of prophylactic costs the Supreme Court has warned cannot be used to 'manufacture' standing, even if those costs are reasonable." *Id.* at 367 (quoting *Clapper*, 568 U.S. at 416). We concluded that a

court order requiring a company to pay damages to "thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses." *Id.* at 368.

The Third Circuit's analysis in *Reilly* and our similar holding in *Storm* pose a seemingly insurmountable hurdle for Plaintiffs Johnson and Palermo. Nonetheless, they urge us to reach a different conclusion here.

Plaintiffs argue that the Amended Complaint "demonstrates that Plaintiffs Johnson and Palermo face a substantial risk of future harm from the Data Breach," which is "sufficient to confer standing." (Doc. 62 at 10). They point to the Amended Complaint's allegations that their card information "was compromised" in the hack and that the purpose of the third-party hack was to "obtain Card Information that could be used to commit fraud or [to sell the information] to other criminal actors." (*Id.* at 10–11). "Indeed," Plaintiffs argue, because Plaintiffs Collins and Lavezza suffered tangible harm as a result of the breach, "the fact that some of the data acquired in the breach has already been used to commit fraud moves the risk of future harm to Plaintiffs Johnson and Palermo out of the realm of speculation into the realm of sufficiently imminent and particularized." (*Id.* at 11).

Plaintiffs attempt to distinguish the injuries claimed by Plaintiffs Johnson and Palermo from the injuries alleged in *Reilly* and *Storm*. Plaintiffs argue that

they have alleged "exactly what was missing from the *Reilly* complaint: that the hackers who accessed Rutter's payment card processing system actually stole sensitive Card Information that was already misused to make fraudulent charges to Plaintiffs Collins's and Lavezza's financial accounts." (*Id.* at 12). Similarly, Plaintiffs argue that the dispositive fact in *Storm* was that *none* of the plaintiffs there had experienced fraud or identity theft because of the breach, while two out of four Plaintiffs here have actually been harmed. (*Id.*). Therefore, so the argument goes, because two other plaintiffs suffered an actual injury, the risk that Plaintiffs Johnson and Palermo will too is not speculative, but actual and imminent. (*Id.* at 12–13).

We are not persuaded. As a fundamental matter, Plaintiffs forget that we do not dispense standing "in gross." *See Town of Chester, N.Y. v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (U.S. 2017) (quoting *Davis v. Federal Election Comm'n*, 554 U.S. 724, 734 (2008)). Plaintiffs' argument would require us to grant standing to a plaintiff who is entirely without an injury based solely on the injuries allegedly suffered by a separate plaintiff. That we cannot do.

Moreover, while Plaintiffs point to decisions in the District of Maryland and the Northern District of California in support of this argument, Plaintiffs overlook that the law in the Third Circuit post-*Reilly* is settled. As the District Court in *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459

(D. Md. 2020) explained, the Sixth,[1] Seventh,[2] and Ninth[3] Circuits have accepted that "an increased risk of identity theft *is* sufficient to establish injury-in-fact," while "[i]n contrast, the First[4] and Third[5] Circuits found that an increased risk of identity theft *did not* constitute injury-in-fact." 440 F. Supp. 3d at 458 (emphasis added). Meanwhile, the Fourth Circuit has taken an approach somewhere between those two poles—where a plaintiff alleges that personal information was actually targeted or misused in the hack, then a compromised plaintiff's risk of future injury is sufficiently imminent and non-speculative. *Id.* at 458–60 (citing *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) and *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018)). Plaintiffs may find the law in other circuits persuasive, and we certainty see the logic espoused by those judges. But the Third Circuit has explicitly concluded that the injuries alleged by Plaintiffs Johnson and Palermo—an increased risk of future harm due to a data breach— are insufficient for Article III standing.

Moreover, Plaintiffs read *Reilly* far too narrowly. While the Fourth Circuit seems to envision a balancing test of sorts, see *In re Marriott Int'l*, 440 F. Supp. 3d at 458–60, the Third Circuit drew a bright line—"allegations of an increased risk of

---

1 *See Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384, 387–89 (6th Cir. 2016).
2 *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694–95 (7th Cir. 2015).
3 *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010).
4 *See Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012).
5 *See Reilly*, 664 F.3d at 40.

identity theft resulting from a security breach are [] insufficient to secure standing." *Reilly*, 664 F.3d at 43; *see also In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 641 (3d Cir. 2017) (Shwartz, J., concurring) ("[U]nder our precedent, a risk of identity theft or fraud is too speculative to constitute an injury in fact.").

We understand that the *Reilly* plaintiffs could not allege *any* misuse of *anyone's* stolen information, while here there was at least *some* misuse of *some* people's information. But this distinction relies on a strained interpretation of *Reilly*. The *Reilly* plaintiffs' allegations of future injury relied "on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names." *Id.* at 42. The Third Circuit noted this was too conjectural: "Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm." *Id.*

Plaintiffs somehow read this discussion to say that if there had been *any* information improperly accessed and used by the hacker, then a presently uninjured person whose information was hypothetically compromised does not suffer too speculative an injury. But *Reilly* was clear: "The District Court correctly

held that Appellants failed to plead specific facts demonstrating they have standing to bring this suit under Article III, because Appellants' allegations of an increased risk of identity theft as a result of the security breach are hypothetical, future injuries, and are therefore insufficient to establish standing." *Id.* at 46. In other words, even if some information was misused by the hacker, it is still speculative to assume someone else's information will be misused as well. The Third Circuit was unequivocal—where a plaintiff suffers no actual injury in a data breach, that plaintiff cannot rely on the mere possibility of future injury to establish standing.

As in *Reilly*, the harm that Plaintiffs Johnson and Palermo may face in the future—even if that harm is arguably more likely to occur than in *Reilly*—depends on multiple levels of impermissible speculation. To hold here that a plaintiff in a data breach class action, who has presently suffered no cognizable injury, can establish standing with allegations that she suffers some unquantifiable risk of future harm based on the lone fact that *other* people were harmed would totally undermine *Reilly*'s bright-line rule. There may be a current—and perhaps widening—split among the circuit courts, but that does not persuade us to reach any other conclusion than the one we are compelled to reach pursuant to *Reilly*. Plaintiffs Johnson and Palermo allege only possible future injuries and prophylactic measures to avoid those potential injuries, neither of which confer

standing in a data breach action brought in the Third Circuit. Because they lack standing, they must be dismissed from this case.

B. Plaintiffs Have Stated a Negligence Claim

Under Pennsylvania law, "[i]t is axiomatic that in order to maintain a negligence action, the plaintiff must show that the defendant had a duty to conform to a certain standard of conduct; that the defendant breached that duty; that such breach caused the injury in question; and actual loss or damage." *Wisniski v. Brown & Brown Ins. Co.*, 906 A.2d 571, 575–76 (Pa. Super. Ct. 2006) (quoting *Phillips v. Cricket Lighters*, 841 A.2d 1000, 1008 (Pa. 2003)). The parties here only dispute the first prong—whether Rutter's owed Plaintiffs any cognizable duty. That question is matter of law for the court to decide. *See R.W. v. Manzek*, 888 A.2d 740, 746 (Pa. 2005). "In negligence cases, a duty consists of one party's obligation to conform to a particular standard of care for the protection of another. This concept is rooted in public policy." *Id.* "Negligence is the absence of ordinary care that a reasonably prudent person would exercise in the same or similar circumstances." *Walters v. UPMC Presbyterian Shadyside*, 187 A.3d 214, 221 (Pa. 2018) (quoting *Martin v. Evans*, 711 A.2d 458, 462 (Pa. 1998)).

Plaintiffs allege that Rutter's owed a duty to Plaintiffs and class members "to use reasonable means to secure and safeguard the[ir] Card Information and to prevent disclosure of the information to unauthorized individuals." (Doc. 30 at ¶

92). This duty "included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner." (*Id.*). Plaintiffs allege that this duty arose pursuant to "common law, industry standards, card network rules, and representations made in [Rutter's] own privacy policy to keep consumers' Card Information confidential and to protect it from unauthorized access." (*Id.* at ¶ 39).

Rutter's argues that it owed no such duty under Pennsylvania law: "No Pennsylvania court has imposed tort duties under the facts of this case: a consumer voluntarily choosing to purchase goods from a retailer and voluntarily choosing a certain method of payment despite being able to pay for goods by other means with no risk of the consumer's alleged harm." (Doc. 46 at 16). Rutter's argument is straightforward: because Pennsylvania law has never explicitly imposed a duty on retailers to safeguard consumers' credit and/or debit card information, Plaintiffs' negligence claim must fall as a matter of law. (*Id.* at 17).

Plaintiffs counter by pointing to the Pennsylvania Supreme Court's 2018 decision in *Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018). In *Dittman*, UPMC employees brought a putative class action against the medical center following a data breach, where the employees' personal and financial information—information entrusted to UPMC as a condition of their employment—was compromised. *Dittman*, 196 A.3d at 1038–40. Plaintiffs' negligence claim

featured two key allegations in support of the duty prong: first, that UPMC had a duty to exercise reasonable care to protect the information that was within its possession or control—in other words, UPMC took an affirmative action (collecting and storing the information) and a duty followed (protecting that information). *Id.* at 1039. Plaintiffs also alleged that UPMC had undertaken a duty of care because of the "special relationship" between the parties, since plaintiffs had to provide the information as a condition of their employment. *Id.* A state trial court and an appellate court panel both agreed that courts should not impose a new duty of care that would allow plaintiffs to recover damages in data breach actions based on common law negligence claims. *Id.* at 1039–43. Both courts looked to *Althaus ex rel. Althaus v. Cohen*, 756 A.2d 1166 (Pa. 2000), where the Pennsylvania Supreme Court delineated a five-factor test to determine whether a court should recognize a new duty of care.[6] *Id.* Applying the *Althaus* factors, both lower courts declined to recognize a new, affirmative duty on entities storing confidential information to protect that information from criminal acts of third parties. *Id.*

[6] "The determination of whether a duty exists in a particular case involves the weighing of several discrete factors which include: (1) the relationship between the parties; (2) the social utility of the actor's conduct; (3) the nature of the risk imposed and foreseeability of the harm incurred; (4) the consequences of imposing a duty upon the actor; and (5) the overall public interest in the proposed solution." *Althaus*, 756 A.2d at 1169.

On appeal, the Pennsylvania Supreme Court reversed. The court disagreed that plaintiffs were seeking to impose a "new, affirmative duty requiring analysis of the *Althaus* factors." *Id.* at 1046. Rather, the case involved the "application of an existing duty to a novel factual scenario." *Id.* The court had already recognized that, consistent with Section 302 of the Restatement (Second) of Torts, "[i]n scenarios involving an actor's affirmative conduct, he is generally 'under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.'" *Id.* at 1046–47 (quoting *Seebold v. Prison Health Services, Inc.*, 57 A.3d 1232, 1246 (Pa. 2012)). Because UPMC had required plaintiffs to provide certain personal and financial information, which it collected and stored on its computer systems (allegedly without adequate security measures in place), the "factual assertions plainly constitute affirmative conduct on the part of UPMC." *Id.* at 1047. While defendants normally do not owe a duty to protect against unforeseen risks, plaintiffs had sufficiently pled that UPMC's affirmative conduct had created a foreseeable risk of data breach, and so UPMC owed them a "duty to exercise reasonable care to protect against an unreasonable risk of harm rising out of that act." *Id.*

Defendant Rutter's contends that *Dittman*'s holding is much narrower—it argues that the sole duty recognized there was "based on the existence of a special

relationship between the parties, i.e. employment relationship, and the fact that employees were required to provide personal information to the employer as a condition of employment." (Doc. 64 at 4–5). According to Rutter's, since there is no special relationship alleged here and because Plaintiffs were not *required* to pay with a credit or debit card, *Dittman* provides no basis to impose a similar legal duty on Rutter's. (*Id.* at 5).

We disagree with Rutter's limited reading of *Dittman*. It is certainly true that *Dittman* involved an employer-employee relationship, where the plaintiffs were required to give the defendant certain information as a precondition of employment. It is also true that courts have read *Dittman*'s ultimate holding—that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system," *id.* at 1038—as potentially limited to just this particular factual scenario. *See Fragale v. Wells Fargo Bank, N.A.*, No. CV 20-1667, 2020 WL 4815804, at *5 (E.D. Pa. Aug. 19, 2020), *reconsideration denied*, No. CV 20-1667, 2020 WL 6498653 (E.D. Pa. Oct. 7, 2020) ("However, unlike in *Dittman*, which involved a relationship and the duties owed by an employer to its employees, here, there is no relationship (contractual or otherwise) between Wells Fargo and Plaintiff, a noncustomer."). But we understand *Dittman* to support a more general principle that has significant applicability here—that in new factual

scenarios, a court need not undertake the burdensome task of carving out new legal duties, but, instead, courts can and should apply longstanding duties where possible. *See Dittman*, 196 A.3d at 1046 ("[I]t is unnecessary 'to conduct a full-blown public policy assessment in every instance in which a longstanding duty imposed on members of the public at large arises in a novel factual scenario. Common-law duties stated in general terms are framed in such fashion for the very reason that they have broad-scale application.'") (quoting *Alderwoods (Pennsylvania), Inc. v. Duquesne Light Co.*, 106 A.3d 27, 40 (Pa. 2014)).

Indeed, just last year the Pennsylvania Supreme Court clarified that while "*Dittman* may have been our first opportunity to recognize this duty in the context of computer systems security," there was "longstanding jurisprudence" that supported the holding that "[i]n scenarios involving an actor's affirmative conduct, he is generally 'under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.'" *Feleccia v. Lackawanna Coll.*, 215 A.3d 3, 14 (Pa. 2019) (quoting *Dittman*, 196 A.3d at 1046). And Chief Justice Saylor, in a partial concurrence and dissent in *Dittman*, expressed his "difficulty with the majority's framing of the duty in issue . . . in terms of a broader duty of care pertaining to affirmative conduct that runs to the public at large." *Dittman*, 196 A.3d at 1057 n.1 (Saylor, C.J., concurring). Chief Justice Saylor explained that he understood the duty to arise from the parties'

contractual and employment-based special relationship. *Id.* at 1057 n.2 (Saylor, C.J., concurring). The fact that Chief Justice Saylor wrote separately to express his preferred formulation of the duty persuades us that the majority opinion in fact relied primarily on UPMC's affirmative conduct, and not solely the parties' employment relationship. To be sure, that the plaintiffs were required to provide UPMC with the information as a condition of employment was a critical factor, but more so because it signaled clear, affirmative conduct by UPMC—it specifically asked for that information and strove to maintain that information in its computers and databases. *See Feleccia*, 215 A.3d at 14 ("We [recognized the employers' duty in *Dittman*] because UPMC had required its employees to provide sensitive personal information, and then collected and stored that information on its computer system without implementing adequate security measures, such as encryption, firewalls, or authentication protocols. We reasoned that this 'affirmative conduct' by UPMC created the risk of a data breach, which in fact occurred.") (internal citations omitted).

We do not hold that *Dittman* necessarily compels the conclusion that Rutter's owed Plaintiffs a clearly-established duty of care as a matter of law. Instead, *Dittman* merely convinces us that the analysis is not as straightforward as Rutter's frames it. Rutter's may be correct that no Pennsylvania court has *explicitly* recognized a duty of care owed by retail establishments to consumers to

protect their credit and debit card information from criminal data breaches. But as explained in *Dittman*, that is not dispositive, and we need not create a new duty here—we can instead apply pre-established duties to new situations as they arise in our rapidly-evolving society. We therefore must look back to the Amended Complaint to ascertain whether Plaintiffs sufficiently plead a duty of care owed to them by Rutter's based on Rutter's affirmative conduct and the risk of foreseeable harm.

Plaintiffs claim Rutter's "was an active participant in the payment card networks as it collected and likely transmitted thousands (or more) of sets of payment card data per day." (Doc. 30 at ¶ 56). According to Plaintiffs, who ostensibly quote from a previous version of Rutter's website, Rutter's took affirmative action to "retain" certain information, such as credit card data, and "protect" it. (*Id.* at ¶ 46). Rutter's specifically took "security measures to protect against unauthorized access to or unauthorized altercation, disclosure, or destruction of data," including "physical security measures to guard against unauthorized access to its systems." (*Id.*). Such measures are, at least theoretically, consistent with the guidelines promulgated by the PCI DDS, which impose binding rules on all merchants who "store, process, or transmit payment card data." (*Id.* at ¶ 50). Plaintiffs also claim that Rutter's was on notice that a data breach of this magnitude could occur: in November 2019, Visa had warned

gas stations like Rutter's that internal processing systems used at gas stations were being increasingly targeted by hackers. (*Id.* at ¶ 41). And on at least one prior occasion, individuals had sought to steal credit card information at ATMs via the installation of skimping devices at certain Rutter's locations. (*Id.* at ¶ 40).

In all, Plaintiffs allege that Rutter's (1) invited customers to use credit and debit cards at their stores; (2) retained costumers' credit and debit card information, (3) took affirmative steps to protect that information, (4) was on notice that hackers were targeting that information, but (5) failed to implement adequate security measures to protect against the foreseeable risk of a data breach. As explained in *Feleccia*, there is "longstanding jurisprudence" in Pennsylvania that "[i]n scenarios involving an actor's affirmative conduct," the actor is typically "under a duty . . . to protect [others] against an unreasonable risk of harm to them arising out of the act." 215 A.3d at 14 (quoting *Dittman*, 196 A.3d at 1046). While, unlike in *Dittman*, there is no pre-existing "special relationship" between Rutter's and Plaintiffs akin to an employer-employee relationship, a defendant's affirmative conduct can nonetheless be the origin of such a special relationship—in other words, affirmative conduct associated with an increased risk of harm can yield a special relationship for tort purposes. *Id.* at 15 ("Application of these legal principles to the present factual scenario supports a determination that 'affirmative conduct' by appellants created a 'special relationship' with and increased risk of

harm to its student athletes such that appellants had a duty to 'exercise reasonable care to protect them against an unreasonable risk of harm arising' from that affirmative conduct.") (quoting *Dittman*, 196 A.3d at 1046).

Based on Plaintiffs' allegations, we find that Defendant's affirmative act of retaining credit and debit card information which created a risk of foreseeable harm from unscrupulous third parties is enough to recognize a legal duty here. Of course, Rutter's may be able to prove at summary judgment or trial that it satisfied this duty through the maintenance of adequate security measures, but that is not the task before us today. Because duty is the lone negligence element Rutter's challenges in its motion for dismissal, we hold that Plaintiffs have sufficiently stated their negligence claim.[7]

---

[7] Even though we are only concerned with the contours of Pennsylvania law here, it is notable that other federal courts applying their states' respective tort principles have also recognized a legal duty in similar contexts. *See, e.g.*, *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1326 (N.D. Ga. 2019) ("[T]his Court concludes that, under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident."); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) ("Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law.").

Rutter's, for its part, cites to opinions from the Seventh and Eighth Circuits for the opposite—that "[o]ther federal courts have declined to impose common law duties in similar contexts." (Doc. 46 at 16–17) (first citing *In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019); then citing *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 816 (7th Cir. 2018)). But these cases, unlike the decisions in *Equifax* and *Sony Gaming Networks*, are wholly unpersuasive. Both relied on Illinois law, and Illinois state courts have explicitly declined to recognize any duty to safeguard personal information. *See Cmty. Bank of Toronto*, 887 F.3d at 816 ("[W]ith regard to data security, Illinois courts have specifically declined to recognize a

C. Plaintiffs' negligence per se claim (Count II) must be dismissed

Plaintiffs claim that Defendant's data security failures violated Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. (Doc. 30 at ¶¶ 58–62). Section 5 of the FTCA declares as "unlawful" any "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). Plaintiffs allege that Section 5 imposes a legal duty to use reasonable security measures—which Rutter's violated by "failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including PCI DDS"—and that the harm that has occurred is the type that the FTCA intended to guard against. (Doc. 30 at ¶¶ 95, 107–08). Therefore, according to Plaintiffs, Defendants' violation of the FTCA constitutes negligence per se. (*Id.* at ¶ 111).

Rutter's argues that Plaintiffs' negligence per se claim fails as a matter of law because Section 5 of the FTCA does not impose any data security standard, nor is there any allegation that the statute was intended to guard against these types

---

common law duty to safeguard personal information even where such information included social security data and medical information."); *see also In re Marriott Int'l*, 440 F. Supp. 3d at 478 (recognizing that while Illinois law precluded the imposition of a legal duty on company for the negligence claims brought under Illinois law, the plaintiffs alleging negligence under Florida law had adequately stated a claim). Here, by contrast, the Pennsylvania Supreme Court *has* recognized a common-law tort duty to safeguard personal and financial information, at least in certain factual scenarios indicating affirmative conduct and foreseeable risk of harm. *See Dittman*, 196 A.3d at 1046–48; *see also Scampone v. Highland Park Care Center, LLC*, 57 A.3d 582, 599 (Pa. 2012) ("Like any other cause of action at common law, negligence evolves through either directly applicable decisional law or by analogy, meaning that a defendant is not categorically exempt from liability simply because appellate decisional law has not specifically addressed a theory of liability in a particular context.").

of injuries. (Doc. 45 at 17). Moreover, the "fairness" standards elucidated in Section 5 are too broad and flexible to support a negligence per se claim. (*Id.* at 18).

Under Pennsylvania law, negligence per se is a concept that "establishes the elements of duty and breach of duty where an individual violates an applicable statute, ordinance, or regulation designed to prevent a public harm." *Schemberg v. Smicherko*, 85 A.3d 1071, 1074 (Pa. Super. Ct. 2014).[8] Plaintiffs here bring their negligence per se claim as a separate cause of action. Negligence per se, however, is not "an independent basis of tort liability but rather establishes, by reference to a statutory scheme, the standard of care appropriate to the underlying tort." *Cabiroy v. Scipione*, 767 A.2d 1078, 1081 (Pa. Super. Ct. 2001) (quoting *In re Orthopedic Bone Screw Products Liability Litigation*, 193 F.3d 781, 790 (3d Cir. 1999)).

Where a plaintiff alleges negligence and negligence per se as separate causes of action, courts within the Third Circuit routinely dismiss the negligence per se claim as subsumed within the standard negligence claim. *See, e.g.*, *Sipp-Lipscomb v. Einstein Physicians Pennypack Pediatrics*, No. 20-cv-1926, 2020 WK 7353105,

[8] Pennsylvania law imposes four requirements on plaintiffs seeking to state a negligence per se claim: "(1) The purpose of the statute must be, at least in part, to protect the interest of a group of individuals, as opposed to the public generally; (2) The statute or regulation must clearly apply to the conduct of the defendant; (3) The defendant must violate the statute or regulation; (4) The violation of the statute or regulation must be the proximate cause of the plaintiff's injuries." *Schemberg*, 85 A.3d at 1074 (quoting *Mahan v. Am–Gard, Inc.*, 841 A.2d 1052, 1058–59 (Pa. Super. Ct. 2003)).

at *1 (E.D. Pa. Dec. 9, 2020) ("Although the Court finds that Plaintiffs have successfully pleaded negligence per se as a theory of liability, it agrees with Cho that Pennsylvania law does not permit Plaintiffs to plead it as a separate claim from general negligence. As such, it will DISMISS Count VII (Negligence Per Se) but will grant leave for Plaintiffs to amend Count VI (Negligence) to include their theory of negligence per se."); *Simmons v. Simpson House, Inc.*, 224 F. Supp. 3d 406, 417 (E.D. Pa. 2016) ("Several courts in this Circuit have explained, however, that negligence per se is not a separate cause of action, but is instead a theory of liability that supports a negligence claim.") (collecting cases); *Russell v. Chesapeake Appalachia, L.L.C.*, No. 4:14-CV-00148, 2014 WL 6634892, at *3 (M.D. Pa. Nov. 21, 2014) ("While the Plaintiffs attempt to assert both negligence and negligence per se in their Complaint, 'under Pennsylvania law, negligence per se is not a separate cause of action.'") (quoting *Ramsey v. Summers*, No. 10–CV–00829, 2011 WL 811024, *2 (W.D. Pa. Mar.1, 2011) (cleaned up)); *see also Zaborowski v. Hosp. Care Ctr. of Hermitage, Inc.*, 60 Pa. D. & C.4th 474, 498 (Pa. Com. Pl. 2002) ("Since negligence per se is not a separate cause of action, however, the court will not address this argument [whether certain statute may be used as the basis of a negligence per claim] at this time.").

Because we have sustained Count I as sufficiently pled, we find that dismissal of Count II is warranted. *See Simmons*, 224 F. Supp. 3d at 417 ("The

Court dismisses Count 3 against Simpson House because it is subsumed within Counts 1 and 2.").

However, dismissal of Count II does not resolve the central and persisting issue: whether Plaintiffs can actually use Section 5 of the FTCA as a predicate in a negligence per se theory to satisfy the duty and breach elements, as an alternative to the common law duty discussed *supra*.[9] Because Plaintiffs' negligence claim

---

[9] Indeed, it is quite an open question whether a Pennsylvania state court would allow a plaintiff to use Section 5 of the FTCA as the basis of a negligence per se theory.

The Third Circuit has previously concluded that a company can violate Section 5 by failing to maintain adequate data security protocols. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). Several other federal courts, looking to applicable state law negligence schemes, have relied in part on the *Wyndham Worldwide* decision to reject protestations from defendants that the FTCA cannot serve as a negligence per se claim's statutory or regulatory predicate. *See In re Marriott Int'l*, 440 F. Supp. 3d at 481–82; *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 6290670, at *10 (D. Md. Oct. 27, 2020) ("Accenture argues that the FTC Act cannot serve as the predicate for a negligence claim based on the violation of a statute because it does not 'proscribe a particular standard of care.' However, several courts have rejected this argument, finding that data breach plaintiffs adequately had pleaded claims of negligence per se based on alleged violations of Section 5 of the FTC act.") (internal citation omitted); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760–61 (C.D. Ill. 2020) ("[T]he FTC Act can serve as the basis of a negligence per se claim."); *In re Capital One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915, 2020 WL 5629790, at *17–18 (E.D. Va. Sept. 18, 2020) (holding that a negligence per se claim under New York law could be premised on the FTCA, but not under Virginia law, which requires the statute or regulation to be expressly aimed at protecting public safety).

Some federal courts have concluded that other states would disallow a negligence per se claim predicated on Section 5. *See id.*; *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2020 WL 691848, at *9 (M.D. Fla. Jan. 27, 2020) (holding that FTCA cannot be basis of negligence per se claim under Florida law, which squarely forecloses negligence per se claims that rely on a federal statute without a private right of action); *In re Sonic Corp. Customer Data Sec. Breach Litig. (Fin. Institutions)*, No. 1:17-MD-2807, 2020 WL 3577341, at *6 (N.D. Ohio July 1, 2020) ("While the FTC and other courts have interpreted Section 5's terms to apply to data security requirements, the statute's actual terms do not lay out positive, objective standards that, if violated, could give the standard for a negligence per se claim under Oklahoma law.").

will proceed regardless, we need not reach a decision on the viability of this alternative theory of negligence today. Summary judgment or pre-trial motion practice are more appropriate vehicles to analyze the applicability of the FTC Act as a predicate for a Pennsylvania negligence per se claim than the motion *sub judice*, especially because a decision in favor of Rutter's on this point would not dispose of the underlying negligence claim. Defendants are sufficiently on notice that Plaintiffs seek to employ a negligence per se theory at trial to establish the duty and breach prongs of their negligence claim; even with dismissal of Count II, Paragraphs 58 through 62 of the Amended Complaint, which allege that Rutter's violated Section 5 of the FTC Act, remain intact. However, if Plaintiffs wish to amend the operative complaint to ensure the negligence per se theory is fully imbedded in Count I, we would grant leave to file accordingly.

Only one Pennsylvania court has addressed whether Section 5 can support a negligence per se claim, but that court did not analyze the claim pursuant to the specific elements of Pennsylvania law. *See First Choice Fed. Credit Union v. Wendy's Co.*, No. CV 16-506, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017), *report and recommendation adopted*, No. CV 16-506, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017) ("This Court recognizes that Section 5 has been found to be adequate support for a plausible claim for negligence per se asserted by financial institutions against a retailer whose data breach caused damages to those alleged in the instant case. . . . In light of this holding, we decline to find that Defendants' arguments fail to merit dismissal at this stage. Accordingly, it is recommended that the Motion to Dismiss be denied as to Count II.") (citing *In re Home Depot, Inc.*, MDL Docket No. 2583, 2016 WL 2897520, at *4 (N.D. Ga. 2016)).

In sum, we will dismiss Count II of the Amended Complaint, but without prejudice to Plaintiffs if they wish to employ a negligence per se theory to satisfy the duty and breach elements of Count I at a later time.

D. The Economic Loss Doctrine does not preclude Plaintiffs' negligence claim

Rutter's argues that Plaintiffs' negligence claims must be dismissed pursuant to the economic loss doctrine. (Doc. 46 at 19). Under Pennsylvania law, the economic loss doctrine provides that a plaintiff cannot maintain a tort action premised on the breach of a legal duty that arises solely from a contract. *See Dittman*, 196 A.3d at 1054. In other words, the applicability of the economic loss doctrine "turns on the determination of the source of the duty plaintiff claims the defendant owes." *Id.* (quoting *Bilt-Rite Contractors, Inc. v. The Architectural Studio*, 866 A.2d 270, 288 (Pa. 2005)). Where the alleged duty "arises under a contract between the parties, a tort action will not lie from a breach of that duty," and instead, the plaintiff must recover under contract law. *Id.* "However, if the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action." *Id.* (citing *Bilt-Rite*, 866 A.2d at 288).

Defendant's argument that the economic loss doctrine precludes Plaintiffs' negligence claim is premised on the assertion that "Rutter's did not owe Plaintiffs

any independent legal duty beyond alleged contractual duties related to Plaintiffs' purchase of goods and services from Rutter's." (Doc. 46 at 20). We have already concluded, however, that Plaintiffs adequately pled that Rutter's owed them a common law duty to safeguard their credit and debit card information based on Rutter's affirmative conduct and the foreseeable risk of harm. Because "this legal duty exists independently from any contractual obligations between the parties," the economic loss doctrine is no bar to Plaintiffs' negligence claim. *Dittman*, 196 A.3d at 1056.

E. Plaintiffs have sufficiently pled an implied breach of contract claim

In Count III of the Amended Complaint, Plaintiffs bring a claim for breach of implied contract. (Doc. 30 at ¶¶ 116–26). Plaintiffs allege that they entered into an implied contract with Rutter's when they provided their credit and/or debit card information in exchange for Rutter's goods and services. (*Id.* at ¶ 117). In that transaction, according to Plaintiffs, Rutter's impliedly promised to safeguard their card information (as evidenced in part by the representations in Rutter's privacy policy), and Plaintiffs "reasonably believed and expected that Rutter's would use part of" the money paid by Plaintiffs "to obtain adequate data security," which Rutter's failed to do. (*Id.* at ¶¶ 120–21). If they had known that Rutter's would not have kept their "implied promise to keep the Card Information reasonably

secure," then Plaintiffs "would not have provided their Card Information to Rutter's." (*Id.* at ¶ 122).

In Pennsylvania, a claim for breach of contract requires "(1) the existence of a contract, including its essential terms, (2) a breach of a duty imposed by the contract, and (3) resultant damages." *CoreStates Bank, N.A. v. Cutillo*, 723 A.2d 1053, 1058 (Pa. Super. Ct. 1999). "The essential elements of breach of implied contract are the same as an express contract, except the contract is implied through the parties' conduct, rather than expressly written." *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015), *aff'd sub nom. Enslin v. Coca-Cola Co.*, 739 F. App'x 91 (3d Cir. 2018) (citing *Highland Sewer & Water Auth. v. Forest Hills Mun. Auth.*, 797 A.2d 385, 390 (Pa. Commw. Ct. 2002). Intent can be "gleaned from the parties' ordinary course of dealing," but "naked assertions devoid of further factual enhancement fail to state an actionable claim." *Longenecker-Wells v. Benecard Services Inc.*, 658 F. App'x. 659, 662 (3d Cir. 2016).

Rutter's argues that Plaintiffs fail to establish the necessary elements for breach of implied contract under Pennsylvania law. (Doc. 46 at 21–25). Specifically, Rutter's asserts that no "meeting of the minds" between Plaintiffs and Rutter's occurred. Despite Plaintiffs' allegations that "Rutter's agreed to take reasonable steps to protect the Card Information," (Doc. 30 at ¶ 117), Rutter's says

there is insufficient factual basis for that "assumption." (Doc. 46 at 22). Rutter's points to the Third Circuit's decision in *Longenecker-Wells*, where the Court rejected an implied breach of contract claim premised on the entrustment of confidential information as a condition of employment or doing business with the company-defendant. *Longenecker-Wells*, 658 F. App'x at 662. By contrast, argues Rutter's, Plaintiffs were not required to provide Rutter's any personal information before making a purchase, which makes the implied contract claim here even less surefooted than in *Longenecker-Wells*. Further, Plaintiffs' reliance on Rutter's privacy policy is misplaced because "they do not allege that they read or were even aware of the policy" when they purchased products from Rutter's. (Doc. 46 at 24). In all, according to Rutter's, "Pennsylvania precedent makes clear that the reasonable expectations of both parties at the time of the transaction, not the post-hoc, unilateral expectations of one party, are necessary to support the existence of an implied contract." (*Id.* at 25).

We agree with Rutter's that *Longenecker-Wells* is instructive. There, plaintiffs—former employees and customers of defendant—sued a pharmacy benefit administrative services company following a data breach by unknown third parties. *Longenecker-Wells*, 658 F. App'x at 660. Plaintiffs, as a prerequisite to employment or use of the company's services, had provided Benecard with certain personal and financial information that was eventually compromised in the breach.

Id. Judge Caldwell, our late colleague, granted the defendant's motion to dismiss, holding in part that plaintiffs had failed to state their claim for breach of implied contract. *Id.* at 660–61.

The Third Circuit affirmed, explaining that the plaintiffs had "failed to plead any facts supporting their contention that an implied contract arose between the parties other than that Benecard required Plaintiffs' personal information as a prerequisite to employment." *Id.* at 662. This alone, however, did not amount to a "contractual promise to safeguard that information, especially from third party hackers." *Id.* By contrast to the *Enslin* case from the Eastern District, where the plaintiff survived dismissal by referencing concrete examples of the defendant-company's implied promises to safeguard personal information—like privacy policies, codes of conduct, company security practices, etc.—the plaintiffs in *Longenecker-Wells* did not "plead any company-specific documents or policies from which one could infer an implied contractual duty to protect Plaintiffs' information." *Id.* at 662–63 (citing *Enslin*, 136 F. Supp. 3d at 675). A lone allegation that "an implied contract arose 'from the course of conduct'" between plaintiffs and the defendant was "insufficient to defeat a motion to dismiss." *Id.* at 663.

While instructive, however, we do not think *Longenecker-Wells* provides much support for Rutter's here. There, plaintiffs relied *solely* on the fact that they

provided the compromised information to the company as a condition of employment or business. Here, Plaintiffs submit more than mere conclusory allegations—they allege that Rutter's invited Plaintiffs to use their credit and debit cards at its establishments and that Rutter's privacy policy, at least prior to the data breach, said it "take[s] security measures to protect against unauthorized access to or unauthorized alteration, disclosure, or destruction" of the consumer data that Rutter's "maintain[s]." (Doc. 30 at ¶¶ 46–47, 118). Like in *Enslin*, Plaintiffs have referenced company-specific documents and policies to support a promise implied by the parties' conduct. *See Longenecker-Wells*, 658 F. App'x at 662–63 ("Plaintiffs here [in contrast to *Enslin*] do not plead any company-specific documents or policies from which one could infer an implied contractual duty to protect Plaintiffs' information.").

While Rutter's is correct that Plaintiffs were not Rutter's employees and were not mandated to provide their credit and debit card information before purchasing goods, we do not place much weight on this distinction. This is especially so where Plaintiffs plausibly allege that Rutter's made certain express or implied assurances that their data would be safe in Rutter's hands. There are also key differences between an employer-employee relationship and a merchant-consumer relationship. While *Dittman* held that an employer may have a common law duty to protect personal information in certain settings, the Pennsylvania

Supreme Court did not address whether an implied contract also arises in those circumstances.[10] As Judge Leeson eventually explained on summary judgment in the *Enslin* case:

> In some contexts . . . it may readily be seen that an obligation on the part of the bank or merchant to use reasonable measures to safeguard a customer's sensitive information is part of the bargain. . . . But the same cannot be said when an employee provides personal information to an employer as part of the hiring process. The "common understanding" of employers and employees is ***not*** that a contract arises at that moment that obligates the employer to use certain measures to safeguard the employees' information[.] . . . The fact that Coca-Cola had detailed information security policies that its employees were required to follow when handling company data does not alter the picture because, as explained, those rules clearly existed for the purpose of protecting the company from harm, not to inure to the employees' benefit.

Enslin v. Coca-Cola Co., No. 2:14-CV-06476, 2017 WL 1190979, at *14 (E.D. Pa. Mar. 31, 2017) (emphasis added) (internal citations omitted). In other words, the context in which a consumer entrusts data to a merchant may be more suggestive of a promise to secure that data than in an employer-employee relationship. The

[10] The trial court had dismissed the employee-plaintiffs' implied breach of contract claim, and the Superior Court affirmed, without appeal of the issue to the Pennsylvania Supreme Court. *See Dittman*, 196 A.3d at 1040 n.3. The Superior Court found that the employees "did not allege any objective manifestations of UPMC's intent to enter into a contract to protect their information." *Dittman v. UPMC*, 154 A.3d 318, 326 (Pa. Super. Ct. 2017), *vacated*, 196 A.3d 1036 (Pa. 2018). The Superior Court also said that "Appellants did not give their information to UPMC for the consideration of its safe keeping, but instead, for employment purposes." *Id.* Here, by contrast, Plaintiffs alleged that Rutter's objectively manifested an intent to promise the safeguarding of their information by reference to Rutter's privacy policy and they adequately allege consideration. (Doc. 30 at ¶ 121) ("Plaintiffs and class members paid money to Rutter's to purchase items at Rutter's convenience stores and gas at Rutter's gas pumps. Plaintiffs and class members reasonably believed and expected that Rutter's would use part of those funds to obtain adequate data security. Rutter's failed to do so.").

merchant and consumer are engaged in a momentary transaction that features all sorts of unspoken assurances between the parties—that the goods sold are as advertised and that the tender paid is valid, for example. An employer-employee relationship comes with its own unique set of promises and legal responsibilities, but it is an inherently less transactional relationship than that between a retailer and customer. An employment relationship is also usually a formal one, complete with paperwork and express agreements (which likely contain merger and/or integration clauses) between the parties. And personal or financial information provided to an employer is likely to serve a multitude of purposes—to run background checks on potential employees, to set up direct-deposit, to enroll in a retirement or pension plan, etc. When a customer provides financial information to a merchant, however, the customer could fairly assume that the data is for a single, limited purpose and thus the information will not be unreasonably exposed to third-parties; in other words, that the data will be used to complete a transaction and nothing more. Without an implied promise to protect credit and debit card information, a consumer might reasonably decide not to purchase goods from a merchant. Ultimately, it is plausible that a jury could find an implied promise to safeguard financial information provided to the merchant for the limited purchase of effectuating a transaction, especially where the merchant has previously

acknowledged the sanctity of that consumer data in its own documents and public-facing representations.

While Plaintiffs may not ultimately succeed on their implied breach of contract claim, we find that they have pled enough to at least survive dismissal. Other federal district courts—including us, when we sat by designation in the District of Delaware—have reached the same conclusion in similar contexts. As the First Circuit explained:

> When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.

Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011). In *Bray v. GameStop Corp.*, No. 1:17-CV-1365, 2018 WL 11226516 (D. Del. Mar. 16, 2018), where we adjudicated a similar data breach case, we found the First Circuit's analysis in *Anderson* persuasive. We noted how plaintiffs "specifically allege[d] that GameStop's privacy policy . . . suggest[ed] an acknowledgment that data security was known by both sides to be an important factor in using a credit or debit card to make purchases." *Bray*, 2018 WL 11226516, at *6. "Although [plaintiffs'] allegations [were] thinly pled," we decided it was "prudent to proceed with caution at this early stage, especially with the lack of consensus among the

courts"—and so we held that plaintiffs had "sufficiently pled the existence of an implied contract" and that "dismissal [was] inappropriate." *Id.* at *6.

Other courts have concluded the same. *See, e.g., Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1070 (C.D. Ill. 2016) ("When the customer uses a credit card for a commercial transaction, he intends to provide the data to the merchant, and not to an unauthorized third party. . . . There is an implicit agreement to safeguard the customer's information to effectuate the contract.") (internal citations omitted); *In re Brinker*, 2020 WL 691848, at *4 ("The majority of federal courts have held that the existence of an implied contract to safeguard customers' data could reasonably be found to exist between a merchant and customer when a customer uses a payment card to purchase goods and services."); *In re Marriott Int'l, Inc.*, 440 F. Supp. 3d 486 (sustaining implied breach of contract claim under Oregon law); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *16–17 (N.D. Ga. Mar. 5, 2018); *Badish v. RBS Worldpay, Inc.*, No. 1:09-CV-0033-CAP, 2010 WL 11570892, at *6–7 (N.D. Ga. Feb. 5, 2010); *In re Michaels Stores Pin Pad Litig.*, 830 F.Supp.2d 518, 528 (N.D. Ill. 2011); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014).

While none of these decisions construed Pennsylvania law in reaching their holdings, we fail to see any material distinction in Pennsylvania law that compels a

different outcome. Indeed, Plaintiffs relied on several out-of-circuit decisions, and Rutter's did not present clear Pennsylvania law to the contrary that dissuades us from considering these persuasive opinions.

Of course, the federal courts are not unified on this issue. We are aware that some courts have reached different conclusions. *See Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015); *In re Zappos.com, Inc.*, No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013). But as we explained in *Bray*, rather than compel a different outcome, these other opinions serve to underscore how the law is still unsettled in many states. This is especially so for us, since neither the Third Circuit nor the Pennsylvania Supreme Court has yet to explicitly answer whether a consumer data breach class action can ever maintain a viable breach of implied contract claim.

Rutter's certainly has a reasonable argument that no implied contract ever materialized. But, as in *Bray*, and considering the absence of any binding law to the contrary, we find it prudent to allow Plaintiffs' breach of implied contract claim to proceed.

F. Plaintiffs have adequately stated an unjust enrichment claim

Plaintiffs' fifth claim, pled in the alternative to Count III, is for unjust enrichment. To state a claim for unjust enrichment under Pennsylvania law, a plaintiff must allege (1) that the plaintiff conferred a benefit on the defendant; (2) the defendant appreciated the benefit; and (3) the defendant accepted and retained the benefit under circumstances in which it would be inequitable to do so without paying for the benefit. *Karden Constr. Servs., Inc. v. D'Amico*, 219 A.3d 619, 628 (Pa. Super. Ct. 2019).

Plaintiffs allege that they (and the putative class members) "conferred a material benefit upon Rutter's in the form of monies paid for the purchase of food and food-related services at its locations." (Doc. 30 at ¶ 145). The monies that Plaintiffs paid to Rutter's "were supposed to be used by Rutter's, in part, to pay for adequate data privacy infrastructure, practices, and procedures.") (*Id.* at ¶ 147). Plaintiffs allege that Rutter's "should not be permitted to retain" that money because Rutter's failed to adequately implement the data privacy and security practices for which Plaintiffs paid. (*Id.* at ¶ 149).

Rutter's argues that Count V must be dismissed as implausibly pled. According to Rutter's, Plaintiffs got exactly "what they actually purchased and what Rutter's actually agreed to provide in exchange for Plaintiffs' payments," which was "food and food-related services." (Doc. 46 at 26). Although Plaintiffs

plead that their purchases "were supposed to be used" for data security practices, Rutter's argues that "Plaintiffs' unilateral beliefs . . . are insufficient to support a claim to unjust enrichment." (*Id.* at 27). Further, Rutter's notes that customers who pay with card pay the same price for goods and services as those who pay with cash, and so Plaintiffs have no basis to assert that they paid extra for data security. (*Id.*).

We adjudicated a similar claim in *Bray v. GameStop*. There, although we were not construing Pennsylvania law, we concluded that plaintiffs plausibly alleged an unjust enrichment claim on the same theory presented here: "based on the allegations, Plaintiffs have plausibly alleged that data security was part of what they paid for but did not receive." *Bray*, 2018 WL 11226516, at *4. Likewise, while Rutter's is correct that Plaintiffs did receive goods and services in exchange for payment, Plaintiffs also allege that they paid for data security. Rutter's decries this allegation as a "bare assertion" that compels dismissal, (Doc. 46 at 27), but we disagree. A plaintiff need only assert plausible allegations at this stage, and considering the fact that Rutter's has previously acknowledged its efforts to maintain and protect customer data, it is plausible that the cost of data security is baked into its prices.

We also in *Bray* rejected the defendant's argument that customers who pay with cash pay the same price as those who use a credit or debit card: "GameStop

argues that the price of its products is the same whether a customer pays with a credit or debit card or with cash, rendering an overpayment theory implausible. While it may be true that all customers, regardless of payment method, pay the same price for GameStop's products, that fact is not before us." *Id.* Likewise here, we can only consider the allegations in the pleadings. While Plaintiffs do not affirmatively plead that they did pay more than cash-paying customers, we will not infer a negative from silence at this stage.

Rutter's is also correct that the goods Plaintiffs received were not defective. But Plaintiffs' "unjust enrichment claim is not directed to the value of the goods received." *Rudolph v. Hudson's Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *12 (S.D.N.Y. May 7, 2019). Rather, the claim is that Rutter's "profited from [Plaintiffs'] purchase[s] but by failing to secure [their] card data," Rutter's "did not provide full compensation for the benefit [the data] provided." *Id.*

Similar to implied breach of contract claims, the federal courts are not uniform in their analyses of unjust enrichment claims in data breach class actions. A court in the District of Minnesota rejected an "overcharge" theory because it construed the silence in the pleadings as to the prices charged to cash and credit customers as evidence that they are charged equally, but that same court sustained the plaintiffs' "would not have shopped" theory. *See In re Target Corp.*, 66 F.

Supp. 3d at 1178 ("If Plaintiffs can establish that they shopped at Target after Target knew or should have known of the breach, and that Plaintiffs would not have shopped at Target had they known about the breach, a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target 'in equity and good conscience' should not have received."). An Oregon court, however, found allegations similar to Plaintiffs' sufficient to withstand dismissal. *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016) ("Plaintiffs allege that they made payments to Premera and that under the circumstances it is unjust for Premera to retain the benefits received without payment. This is sufficient to withstand a motion to dismiss."). A New York federal court concluded the same. *See Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017). Meanwhile, a court in Illinois applying Arizona law rejected an unjust enrichment claim, quipping that the plaintiff only "paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase." *Irwin*, 175 F. Supp. 3d at 1072. The Seventh and Eighth Circuits have shot down similar unjust enrichment claims, while the Eleventh has upheld them. *Compare Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) *and Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016), *with Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

After reviewing the case law, we find that dismissal of unjust enrichment claims in putative data breach class actions ultimately depends on the level of deference a court affords a plaintiff's allegations. For example, the Eighth Circuit in *Carlsen* said that because the plaintiff did not explicitly "allege that any specific portion of his subscriber fee went toward data protection or that GameStop agreed to provide additional protection to paid subscribers that it did not also provide to non-paid subscribers," the plaintiff "alleged neither a benefit conferred in exchange for protection of his [personal information], nor has he shown how GameStop's retention of his subscription fee would be inequitable." *Carlsen*, 833 F.3d at 912. The Eleventh Circuit in *Resnick*, however, sustained the unjust enrichment claim after construing as true plaintiffs' allegations that they conferred a monetary benefit in the form of premiums, the defendant-company appreciated the benefit and used some of the money to pay for data management and security, and that it would be unjust to retain that money without implementation of adequate data security. *Resnick*, 693 F.3d at 1328. An Arizona federal court concluded the same based on plaintiffs' straightforward allegations: "Plaintiffs allege that they paid money to Defendant for insurance plan premiums and healthcare service, that part of the money was supposed to be used for the administrative costs of data security, and that Defendant failed to provide adequate data security. These allegations are sufficient to support a claim for unjust enrichment." *In re Banner Health Data*

Breach Litig., No. CV-16-02696-PHX-SRB, 2017 WL 6763548, at *6 (D. Ariz. Dec. 20, 2017).

The Plaintiffs here plead all elements required to state an unjust enrichment claim. Plaintiffs allege they conferred a benefit to Rutter's in the form of money for goods and services. (Doc. 30 at ¶ 145). Plaintiffs allege Rutter's appreciated these benefits or at least had knowledge that Plaintiffs conferred money upon it. (*Id.* at ¶ 146). And Plaintiffs allege this money was unjustly retained by Rutter's because it was not dedicated towards adequate data security. (*Id.* at ¶ 147). These allegations are certainly thin, but we do not cast them aside here as implausible or too conclusory. This is especially so because Plaintiffs also plead in detail the security measures that merchants like Rutter's are expected to maintain, and we struggle to see how else Rutter's could support an adequate data security apparatus without profits derived from costumer purchases. Though Plaintiffs' theories may not withstand summary judgment, we decline to dismiss the unjust enrichment claim at this stage.

G. Plaintiffs' PA UTPCPL claim must be dismissed

Finally, Rutter's moves for dismissal of Count IV—a claim under the Pennsylvania Unfair Trade Practices and Consumer Protection Law. The UTPCPL provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by . . . this act . . . are

hereby declared unlawful." 73 P.S. § 201-3. The statute "is designed to protect the public from fraud and deceptive business practices." *Pirozzi v. Penskie Olds–Cadillac–GMC, Inc.*, 605 A.2d 373, 375 (Pa. Super. Ct. 1992). It provides a private right of action for "[a]ny person who purchases . . . goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property" because of the seller's unfair or deceptive practices. 73 P.S. § 201-9.2(a). The UTPCPL provides many definitions identifying what constitutes an "an unfair or deceptive practice," but the catch-all provision defines it as "[e]ngaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or misunderstanding." 73 P .S. § 201-2(4)(xxi).

To maintain a private right of action under the UTPCPL, "a plaintiff must show that he justifiably relied on the defendant's wrongful conduct or representation and that he suffered harm as a result of that reliance." *Yocca v. Pittsburgh Steelers Sports, Inc.*, 854 A.2d 425, 438 (Pa. 2004); *see also Hunt v. U.S. Tobacco Co.*, 538 F.3d 217, 221 (3d Cir. 2008). A plaintiff must also show that she suffered "an ascertainable loss as a result of the defendant's prohibited action." *Weinberg v. Sun Co., Inc.*, 777 A.2d 442, 446 (Pa. 2001).

Plaintiffs allege that the data security failures that precipitated the data breach amounted to unfair or deceptive acts and practices in violation of the

UTPCPL. (Doc. 30 at ¶¶ 127–141). Rutter's argues that Count IV must be dismissed for three reasons: (1) because Plaintiffs fail to plead fraud with the requisite particularly pursuant to Fed. R. Civ. P. 9(b); (2) because Plaintiffs have not alleged an ascertainable loss; and (3) because Plaintiffs have not alleged justifiable reliance. (Doc. 46 at 28–33). We consider each in turn.

a. Rule 9(b)

While plaintiffs who allege fraudulent practices under the UTPCPL must meet Rule 9(b)'s particularity standard, complaints that rely on the statute's prohibition of "deceptive" business practices need not. *See, e.g., Schnell v. Bank of New York Mellon*, 828 F.Supp.2d 798, 807 (E.D. Pa. 2011) (explaining that a plaintiff alleging deceptive acts "therefore does not need to prove all of the elements of common-law fraud or meet the particularity requirement of Federal Rule of Civil Procedure 9(b)").

Here, we find that Plaintiffs do not allege that Rutter's engaged in fraudulent conduct in violation of the UTPCPL. Rather, they claim that "Rutter's engaged in 'unfair methods of competition' or 'unfair or deceptive acts or practices,'" (Doc. 30 at ¶ 131), and explicitly rely on the catch-all provision contained in 73 Pa. Stat. § 201-2(4)(xxi). Deception claims including those under the catch-all provision must only meet the normal pleading standard of Rule 8(a). *See Landau v. Viridian Energy PA LLC*, 223 F. Supp. 3d 401, 418 (E.D. Pa. 2016) ("Today, the vast

weight of authority in Pennsylvania holds that a plaintiff can state a claim under the catch-all provision by pleading facts sufficient to support a claim for fraud or deception."). Rutter's first argument for dismissal of Count IV is therefore rejected.

b. Ascertainable loss and justifiable reliance

A plaintiff asserting a UTPCPL claim must sufficiently allege an ascertainable loss that stems from one's justifiable reliance on the defendant's wrongful conduct. *See Kern v. Lehigh Valley Hosp., Inc.*, 108 A.3d 1281, 1290 (Pa. Super. Ct. 2015) ("Appellant had to demonstrate that he and all prospective class members justifiably relied on Appellee's alleged violations of the UTPCPL and, as a result of those alleged violations, suffered an ascertainable loss."). "To allege an ascertainable loss, the plaintiff 'must be able to point to money or property that he would have had but for the defendant's fraudulent actions.'" *Riviello v. Chase Bank USA, N.A.*, No. 3:19-CV-0510, 2020 WL 1129956, at *3 (M.D. Pa. Mar. 4, 2020) (quoting *Benner v. Bank of Am., N.A.*, 917 F. Supp. 2d 338, 359 (E.D. Pa. 2013)). These damages must be identifiable and "cannot be speculative." *Jarzyna v. Home Properties, L.P.*, 185 F. Supp. 3d 612, 626 (E.D. Pa. 2016), *aff'd*, 783 F. App'x 223 (3d Cir. 2019).

Rutter's argues that Plaintiffs do not allege an ascertainable loss, as they "largely focus on lost time." (Doc. 46 at 31). To the extent Plaintiffs' accounts

were fraudulently comprised by the hacker(s), there is no allegation that their banks failed to reimburse them. (*Id.*). Plaintiffs counter that while their losses might appear minor, they are nonetheless identifiable—both Plaintiffs Collins and Lavezza each spent certain quantities of time and money addressing the breach. (Doc. 62 at 28–29).

Upon closer inspection, it appears that only Plaintiff Lavezza pleads a quantifiable amount of money he lost due to the data breach—multiple overdraft fees from his checking account, plus approximately one full day of work due to various remedial actions, with lost wages at or around $15 per hour. (Doc. 30 at ¶ 16). While Plaintiff Collins dedicated approximately five hours "dealing with" the breach through various "remedial actions," there is no allegation that he lost any money as a result. (*Id.* at ¶ 10). Both Collins and Lavezza were ultimately reimbursed by their banks after fraudulent charges appeared on their cards. (*Id.* at ¶¶ 10, 15). But the statute requires a plaintiff to have suffered a "loss of money or property, real or personal," and only Plaintiff Lavezza has pled a tangible loss of money. 73 P.S. § 201–9.2. Therefore, only Plaintiff Lavezza is able to satisfy this element of a valid UTPCPL claim.[11]

[11] Plaintiffs cite to *Dibish v. Ameriprise Fin., Inc.*, 134 A.3d 1079, 1089 (Pa. Super. Ct. 2016) for the proposition that losing one's "benefit of the bargain" might suffice as an ascertainable loss. But this argument is not supported by that case. *Dibish* concerned a UTPCPL claim arising out of a sale of a life insurance policy. *Dibish*, 134 A.3d at 1083. In short, the plaintiff purchased a policy with a $50,000 benefit under the impression she could pay a monthly

For both Plaintiffs, however, their UTPCPL claim ultimately fails on the "justifiable reliance" prong. To state a claim under the UTPCPL, a plaintiff must show that she "justifiably relied on the defendant's wrongful conduct." *Yocca*, 854 A.2d at 438 (citations omitted). Here, Plaintiffs' complaint only includes a single, conclusory allegation that "Plaintiffs relied on Rutter's misrepresentations and omissions relating to its data privacy and security." (Doc. 30 at ¶ 135). Plaintiffs do, as we have discussed, make certain allegations pertaining to Rutter's privacy policy and that "Plaintiffs and class members provided their Card Information to Rutter's with the reasonable expectation that Rutter's would comply with its obligations to keep the card information confidential and would secure it from

---

premium of $715, but then learned post-purchase that she needed to pay a $1,360 premium to actually obtain that benefit. *Id.* at 1084. The trial court determined the plaintiff's actual damages to be $5,000, but plaintiff appealed, arguing that the compensation should be, at a minimum, for the difference in value between what was bargained for and what was received (calculated by multiplying the difference in premium amounts by the number of years the policy would be in force). *Id.* at 1083–84. The Superior Court affirmed. The court observed that while "no precise definition of actual damages currently prevails, it is clear that a successful plaintiff is entitled to the benefit of her bargain." *Id.* at 1089. By that, court *did not* mean that the abstract "benefit of the bargain" could constitute an ascertainable loss on its own. Rather, the Superior Court was merely affirming the general notion that "actual damages" under the UTPCPL may be difficult to ascertain, and so there must be some "flexibility in calculating actual damages, as they are dependent upon the evidence accepted and found persuasive by a fact-finder." *Id.* The "trial court acknowledged that calculating Appellant's actual damages with precision was difficult because of the underlying flexibility in policy investments, the scheduled premiums, and the death benefit," but the trial court appropriately strove to provide the benefit of the bargain by compensating the plaintiff an amount of money that ensured she received a $50,000 benefit at the price she expected. *Id.* Critically, there was no dispute that plaintiff had suffered an ascertainable loss—the issue was how to precisely calculate that loss in a way that ensured the plaintiff received what she expected based on the defendant's UTPCPL violations. *Id.* at 1087. *Dibish* provides no support for the notion that merely losing the benefit of one's bargain without an identifiable or tangible loss of any kind can sustain a UTPCPL claim.

unauthorized access." (*Id.* at ¶ 47). But we also deem that too conclusory to be considered true at this stage, for Plaintiffs fail to *explicitly* plead their reliance on the privacy policy itself or any other representations made by Rutter's on the subject. *See Weinberg*, 777 A.2d at 446 ("There is no authority which would permit a private plaintiff to pursue an advertiser because an advertisement might deceive members of the audience and might influence a purchasing decision when the plaintiff himself was neither deceived nor influenced. . . . The statute clearly requires, in a private action, that a plaintiff suffer an ascertainable loss *as a result of* the defendant's prohibited action.") (emphasis in original).

Plaintiffs' argument to the contrary does not persuade us otherwise. Plaintiffs attempt to clarify that their UTPCPL claim is "omission-based" and not dependent any "affirmative misrepresentations" by Rutter's "that Plaintiffs relied upon in deciding to make purchase at Rutter's." (Doc. 62 at 30). Therefore, Plaintiffs argue, Rutter's "failure to disclose its data security shortcomings" was a material omission in violation of the UTPCPL. (*Id.*). In support of this argument, Plaintiffs cite to *Drayton v. Pilgrim's Pride Corp.*, No. 03-2334, 2004 WL 765123 (E.D. Pa. Mar. 31, 2004). *Drayton* involved a UTPCPL claim against food processing plants after the plaintiff's husband died from ingestion of contaminated meat products. *Drayton*, 2004 WL 765123, at *1. In addressing the argument that plaintiff's UTPCPL claim did not adequately plead justifiable reliance, Judge

Buckwalter held that in certain scenarios involving a defendant's omission of material information, the reliance element "can be presumed." *Id.* at *7.

There are several flaws with Plaintiffs' argument and reliance on *Drayton*, however. First, to the extent that Plaintiffs claim that their UTPCPL claim does not rely on any affirmative misrepresentations by Rutter's, this is difficult to square with the allegations in the Amended Complaint. Plaintiffs pled that "Rutter's *engaged* . . . in the following conduct: (a) *Representing* that its goods and services had characteristics, uses, benefits, and qualities that they did not have . . . (b) *Representing* that its goods and services were of a particular standard or quality when they were of another quality . . . (c) *Advertising* its goods and services with intent not to sell them as advertised . . . (d) *Engaging* in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding." (Doc. 30 at ¶ 131) (emphasis added). After pleading that Rutter's engaged in certain "*misrepresentations **and*** omissions," (*Id.* at ¶ 136) (emphasis added), Plaintiffs cannot now claim that they only meant to challenge the omissions.

Plus, even if Plaintiffs' UTPCPL claim did derive solely from omissions and not any affirmative misrepresentations, *Drayton* does not provide that the "justifiable reliance" prong just vanishes in such a case. Rather, *Drayton* expressly acknowledged that "in normal UTPCPL false advertising claims[,] reliance is required." *Drayton*, 2004 WL 765123, at *7. The court ultimately concluded that

reliance can be presumed in cases where a manufacturer knows of a defect but does not inform any customers, a principle drawn from a Pennsylvania state trial court case featuring a UTPCPL claim against a car manufacturer. *Id.* (citing *Zwiercan v. General Motors Corp.*, 2002 WL 31053838, 58 Pa. D. & C. 4th 251 (Pa. Com. Pl. 2002). The *Zwiercan* court recognized that "when a duty to speak exists [as it does 'when the seller has superior knowledge of a material fact that is unavailable to the consumer'], reliance by the class plaintiffs is implicit and is established by operation of law." *Zwiercan*, 2002 WL 31053838, at *5. Because the car manufacturer was under a duty to reveal any material defects in its cars, and a purchaser may justifiably rely on an omission in this context and assume that the car (specifically, its front seats) is not defective, the *Zwiercan* court found it appropriate to presume that the plaintiff had satisfied the "reliance" element where the manufacture was silent about any defects. *Id.* at 5. Likewise in *Drayton*, Judge Buckwalter found the presumption of reliance appropriate where "Defendants allegedly knew their product was adulterated and therefore dangerous, and would therefore have a duty to advise unsophisticated consumers of that material fact or not advertise their products as being in compliance with USDA and FDA regulations." *Drayton*, 2004 WL 765123, at *7 ("If a manufacturer does not disclose material information it was duty bound to provide, then the customer may be presumed to have relied upon the manufacturer's silence.").

The facts of both *Zwiercan* and *Drayton* make it clear that the "justifiable reliance" element cannot be presumed in this case. Both cases involved manufacturers of potentially-dangerous products who were ostensibly aware that their products had material defects but did not alert any customers. In such a case, a customer cannot rely on any representations because there is no representation—it's the very act of silence that a customer reasonably relies on. When a meat processer says nothing about the safety of its meat, one can justifiably conclude from that silence that the meat contains no harmful bacteria, for example. In this scenario, "actual reliance [on any misrepresentations] cannot be established," and so courts look "to the nature of the parties' relationship and materiality of the statement to establish a presumption of reliance." *Zwiercan*, 2002 WL 31053838, at *4.

The present matter is very much unlike *Zwiercan* and *Drayton*. We are not persuaded that Rutter's can be aptly compared to a car manufacturer or a meat-processing plant. Plaintiffs were not purchasing any potentially-dangerous products. Rutter's was not duty-bound, like a car manufacturer with front seat defects or meat-processer with a listeria outbreak, to alert customers or state or federal officials as to any potential data-security issues.[12] *See also Moore v.*

[12] While we previously concluded that Rutter's was under a legal duty to safeguard credit and debit card information, we do not conclude that the duty necessarily extends to alerting customers as to the potential activities of future third-party hackers.

Angie's List, Inc., 118 F. Supp. 3d 802, 817 n.8 (E.D. Pa. 2015) ("[Plaintiff argues in error that reliance may be presumed in fraud and UTPCPL claims. Our colleagues have presumed reliance only under narrow circumstances not present here, such as securities fraud, [] and manufacturing defects[.]") (internal citations omitted).

Most importantly, however, the plaintiffs in *Zwiercan* and *Drayton* were totally unable to establish the reliance element—in both cases, "the unsophisticated Plaintiff is at the mercy of the Defendant to inform her of a known safety defect." *Id.* at *3. Here, Rutter's did make representations as to its continuing efforts to safeguard personal data—Plaintiffs just cannot establish they actually relied on those representations prior to making purchases at Rutter's (and now claim that those representations are not even part of their UTPCPL claim).[13] And to the extent that the UTPCPL claim is only omissions-based and not reliant on any affirmative misrepresentations, we are not persuaded that a customer can justifiably rely on a convenience store's silence regarding its data security in the same way that a customer can rely on a car manufacturer's silence as to whether the front seats will be adequately secured to the frame of the car. In other words,

[13] Unlike the UTPCPL claim, proof of reliance is not an explicit element of an implied breach of contract claim, and so the absence of an affirmative allegation that Plaintiffs read the privacy policy and relied on it prior to making a purchase at Rutter's was not fatal to the contract claim at this stage.

we question the materiality of the alleged omissions, especially when compared to the omissions in cases where courts have employed the presumption of reliance. *Cf. Hunt v. U.S. Tobacco Co.*, 538 F.3d 217, 228 n.18 (3d Cir. 2008), *as amended* (Nov. 6, 2008) (noting that, in a putative class action concerning anticompetitive behavior of a smokeless tobacco company where the plaintiff seeks to sustain a UTPCPL claim using the presumption of reliance, the plaintiff had "not adequately explained why the alleged misrepresentations [concerning the efficiency of the smokeless tobacco market] in this case are material to a purchasing decision"); *Wilson v. Parisi*, 549 F. Supp. 2d 637, 668 (M.D. Pa. 2008) ("Here, although the Wilsons never saw the [home] appraisal, they relied on the [defendants] to furnish an appraisal that complied with industry requirements and standards. Like the consumer in *Drayton*, the Wilsons were not in a position to know of the existence of any defects. And absent the appraisal, the transaction would not have been consummated, at least not for $185,000."); *Cave v. Saxon Mortg. Servs., Inc.*, No. CIV.A. 11-4586, 2013 WL 460082, at *1 (E.D. Pa. Feb. 6, 2013) (finding that plaintiffs were entitled to presumption of reliance in UTPCPL claim where a loan term sheet deceptively "omitted critical information about the amount of Plaintiffs' balloon payment, an explanation of how this payment would be calculated, and an amortization schedule for Plaintiffs' payments").

In short, we fear that Plaintiffs' interpretation of *Zwiercan* and *Drayton* relaxes the "justifiable reliance" element of a UTPCPL claim far too much, and we are not convinced the two cases should be applied here. Accordingly, we conclude that Plaintiffs are unable to satisfy the justifiable reliance prong and therefore cannot not state a valid UTPCPL claim.

IV. CONCLUSION

For the foregoing reasons, we shall grant in part and deny in part Rutter's Motion to Dismiss.

ACCORDINGLY, IT IS HEREBY ORDERED THAT:

1. Defendant's Motion to Dismiss, (Doc. 45), is **GRANTED** to the following extent:
    a. Plaintiffs Kathleen Johnson and Morgan K. Palermo are **DISMISSED** for lack of standing. The Clerk of Courts is instructed to **TERMINATE** Kathleen Johnson and Morgan K. Palermo from the docket.
    b. Count II of Plaintiffs' Amended Complaint is **DISMISSED WITHOUT PREJUDICE** to Plaintiffs' ability to pursue a negligence per se theory of liability in Count I.
    c. Count IV of Plaintiffs' Amended Complaint is **DISMISSED**.
2. Defendant's Motion to Dismiss is **DENIED** in all other respects.

3. A Case Management Conference **SHALL BE HELD** on February 26, 2021, at a time to be set by future order.

/s/ John E. Jones III
John E. Jones III, Chief Judge
United States District Court
Middle District of Pennsylvania