

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE ACCELLION, INC. DATA
BREACH LITIGATION

Case No. [5:21-cv-01155-EJD](#)

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS**

Re: ECF No. 174

This action arises from two data breaches in December 2020 and January 2021 of Defendant Accellion, Inc., a cloud software company whose file transfer software was widely used by governmental entities, hospitals, universities, law firms, financial institutions, and private companies. Beginning in February 2021, several individual lawsuits were filed against Accellion and its clients that used the vulnerable software at issue, many of which were transferred to and consolidated in this district. Following consolidation and the Court’s appointment of interim lead counsel, Accellion filed the present motion to dismiss the consolidated complaint. ECF No. 174 (“Mot.”). The Court also heard oral arguments on October 19, 2023.

Based on the parties’ written submission and oral arguments, the Court GRANTS IN PART and DENIES IN PART Accellion’s motion to dismiss the consolidated complaint.

I. FACTUAL BACKGROUND

A. Accellion and FTA

Accellion, Inc. is a cloud-based software company that provides an enterprise content firewall that allegedly “prevents data breaches and compliance violations from third party cyber risk.” Consolidated Class Action Compl. (“Compl.”) ¶ 24. In the early 2000s, Accellion

Case No.: [5:21-cv-01155-EJD](#)

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

developed a file sharing transfer software called File Transfer Appliance (“FTA”), which was intended to “facilitate secure, encrypted file sharing that exceeded limits imposed on the size of email attachments.” *Id.* ¶ 25. Accellion’s file transfer services were used by hundreds of companies, private organizations, and government entities. *Id.* ¶ 29. When individuals transact with such entities that use Accellion’s FTA software, they are typically required to provide their private identifying information (“PII”), which is then transferred by Accellion. *Id.* ¶ 30. Accellion’s services are used to securely transfer files containing PII. *Id.* ¶ 31.

In the years preceding December 2020, Accellion allegedly became aware that the FTA product was “nearing the end of its life” and encouraged its customers to switch to a new product, called Kiteworks. *Id.* ¶ 32.

B. The Data Breaches

On December 16, 2020, an Accellion customer was alerted by the FTA’s anomaly detector that unauthorized third parties had exploited the FTA. Compl. ¶ 42. Upon investigation, Accellion confirmed that the FTA software contained two security vulnerabilities, described as SQL Injection and OS Command Execution. *Id.* Between December 16 and December 23, Accellion released two patches to address the vulnerabilities and notified its clients between December 2020 and January 2021. *Id.* ¶ 43.

On January 20, 2021, a second attack occurred, involving two vulnerabilities described as Server-Side Request Forgery and OS Command Execution. Compl. ¶ 47. At this point, Accellion advised its clients to shut down their FTA systems. *Id.*

Plaintiffs allege that these data breaches were the largest breach in 2021 and one of the largest breaches during the last five years. Compl. ¶ 49. The Complaint lists over sixty (60) entities that had used the FTA product and were impacted by the data breaches, which include several state and governmental agencies, hospitals, universities, law firms, financial institutions, and private companies. *Id.* ¶ 59. Over the course of these two attacks, unauthorized actors gained access to significant quantities of personally identifiable information (“PII”), personal health information (“PHI”), and other information from these entities. Compl. ¶ 49.

Plaintiffs are individuals whose private details were exposed to unauthorized actors as a result of these data breaches. Compl. ¶ 1. The information exposed included “names, dates of birth, Social Security numbers, driver’s license numbers and/or state identification numbers, bank account information, employment information, and personal health information,” collectively referred to as Plaintiff’s “personally identifiable information” (“PII”). *Id.* Plaintiffs allege that they have experienced identity theft, fraudulent charges on their bank and credit accounts, temporary bank freezes, and out-of-pocket losses, such as overdraft fees, credit monitoring costs, and credit card reissuance fees. *Id.* ¶¶ 4–15.

C. Procedural History

On February 17, 2021, the earliest filed complaint in this district was filed by Madalyn Brown against Accellion, Inc., asserting one claim of negligence and one claim for violation of the WCPA. ECF No. 1. Since then, several other complaints were filed in this district and others across the country against Accellion, as well as several of its customers including Health Net, Flagstar Bank, and Kroger.

On January 12, 2022, one group of plaintiffs filed a motion for preliminary approval of class-wide settlement in one of the actions in this district. *See Stobbe v. Accellion*, Case No. 5:21-cv-01353-EJD. However, before the motion could be resolved, this Court consolidated nearly all of the related Accellion actions under the present earliest opened docket. ECF No. 83.

On February 10, 2023, the Court appointed interim co-lead class counsel, which did not include the plaintiff group that reached class-wide settlement. ECF No. 143. Following a subsequent investigation, interim class counsel declined to proceed with the class-wide settlement as to Accellion and filed a consolidated complaint. *See* ECF Nos. 167, 170. Accellion filed the present motion to dismiss all claims asserted against them, which has been fully briefed. ECF Nos. 174 (“Mot.”); 181 (“Opp.”); 187 (“Reply”).

On December 19, 2023, the Court heard oral arguments from the parties.

II. LEGAL STANDARD

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests the legal

Case No.: [5:21-cv-01155-EJD](#)

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

sufficiency of the claims alleged in the complaint. *Ileto v. Glock*, 349 F.3d 1191, 1199–1200 (9th Cir. 2003). Under Federal Rule of Civil Procedure 8, a complaint must include a “short and plain statement of the claim showing that the pleader is entitled to relief,” and may be dismissed under Rule 12(b)(6) if the plaintiff fails to state a cognizable legal theory or has not alleged sufficient facts to support such a theory. *Somers v. Apple, Inc.*, 729 F.3d 953, 959 (9th Cir. 2013). When deciding whether to grant a motion to dismiss, the court must generally accept as true all “well-pleaded factual allegations.” *Ashcroft v. Iqbal*, 556 U.S. 662, 664 (2009). The court must also construe the alleged facts in the light most favorable to the plaintiff. *See Retail Prop. Trust v. United Bd. of Carpenters & Joiners of Am.*, 768 F.3d 938, 945 (9th Cir. 2014) (“[The court] must accept as true all factual allegations in the complaint and draw all reasonable inferences in favor of the nonmoving party.”). However, “courts are not bound to accept as true a legal conclusion couched as a factual allegation.” *Iqbal*, 556 U.S. at 678.

The court usually does not consider material beyond the pleadings for a Rule 12(b)(6) motion. *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n. 19 (9th Cir. 1989). Exceptions include material incorporated by reference in the complaint and material subject to judicial notice. *See Lee v. City of Los Angeles*, 250 F.3d 668, 688–69 (9th Cir. 2001).

III. DISCUSSION

Plaintiffs assert eleven claims against Accellion: (1) negligence; (2) negligence per se; (3) violation of the California Consumer Privacy Act; (4) violation of the Confidentiality of Medical Information Act; (5) violation of the California Customer Records Act; (6) intrusion upon seclusion; (7) breach of contract; (8) unjust enrichment; (9) violation of the California Constitution right to privacy; (10) violation of the Washington Consumer Protection Act; and (11) violation of the Michigan Consumer Protection Act (“MCPA”).¹ *See* Compl., ECF No. 170.

As an initial point, Accellion first argues for dismissal due to impermissible group pleading. Mot. 5. However, any ambiguity as to the group references to “Defendants” has largely

¹ Plaintiffs do not oppose dismissal of their MCPA claim. Opp. 2 n.1.

been resolved by the subsequent severance and transfer of all claims against Flagstar to the Eastern District of Michigan, which is the only remaining non-Accellion defendant in this consolidated action. ECF No. 182. Because the Complaint expressly defines “Defendants” as referring to Accellion and the Flagstar entities (Compl. at 1), the Court will evaluate the Complaint’s references to “Defendants” in the complaint as references to Accellion only.

A. Negligence

“To state a claim for negligence in California, a plaintiff must establish the following elements: (1) the defendant had a duty, or an ‘obligation to conform to a certain standard of conduct for the protection of others against unreasonable risks,’ (2) the defendant breached that duty, (3) that breach proximately caused the plaintiff’s injuries, and (4) damages.”

Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1038–39 (N.D. Cal. 2019).

Accellion moves to dismiss Plaintiffs’ negligence claim for failure to allege facts giving rise to a duty of care, breach of any such duty, and cognizable damages. Mot. 5–10. The Complaint alleges that Accellion owed Plaintiffs a duty of reasonable care to preserve and protect the confidentiality of the PII collected, which included maintaining and testing its security systems and taking reasonable security measures to safeguard the PII. Compl. ¶ 116. Plaintiffs allege this duty arose from Accellion’s commitments to its clients (*id.* ¶¶ 65, 116); its role as the “purported expert guardians and gatekeepers of data” (*id.* ¶ 116); its “responsibility to provide data security consistent with industry standards,” such as those under the CCRA, the FTC Act, HIPAA, and COPPA (*id.* ¶¶ 118, 122); the special relationship between Accellion and the end users of the services it provided to its immediate clients (*id.* ¶¶ 119, 120, 140); as well as Accellion’s common law duty to prevent foreseeable harm to others (*id.* ¶ 121).

1. Duty to Protect

Accellion first contends that California law does not impose a general duty on companies to protect against even foreseeable harm by third parties. Mot. 6. Citing *Doe v. Uber Techs.*, 79 Cal. App. 5th 410 (2022), Accellion argues that Plaintiffs do not allege misfeasance, nor does it have a “special relationship” with the Plaintiffs that would permit liability for nonfeasance. *Id.*

Case No.: [5:21-cv-01155-EJD](#)

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Under California law, each person has a general duty ‘to exercise, in his or her activities, reasonable care for the safety of others.’” *Brown v. USA Taekwondo* (“USAT”), 11 Cal. 5th 204, 214 (2021), *reh’g denied* (May 12, 2021); *see also* Cal. Civ. Code § 1714(a). However, “one owes no duty to control the conduct of another, nor to warn those endangered by such conduct.” *Regents of Univ. of California v. Superior Ct.*, 4 Cal. 5th 607, 619 (2018). This “no-duty-to-protect rule is not absolute, however. . . . In a case involving harm caused by a third party, a person may have an affirmative duty to protect the victim of another’s harm if that person is in what the law calls a ‘special relationship’ with either the victim or the person who created the harm.” *USAT*, 11 Cal. 5th at 215.

The California Supreme Court has set forth a two-step inquiry in determining whether to recognize a duty to protect: “First, the court must determine whether there exists a special relationship between the parties or some other set of circumstances giving rise to an affirmative duty to protect. Second, if so, the court must consult the factors described in *Rowland* to determine whether relevant policy considerations counsel limiting that duty.” *USAT*, 11 Cal. 5th at 209 (citing *Rowland v. Christian*, 69 Cal. 2d 108, 113 (1968)).

a. Special Relationship

With respect to the first step of the *USAT* two-step inquiry, the Court finds that there exists a special relationship between a file transfer company and the individuals whose information is being transferred.

In *Regents of Univ. of California v. Superior Ct.*, 4 Cal. 5th 607 (2018), the California Supreme Court described the features of a special relationship that would permit the law to impose a duty to protect on one of the parties to the relationship. The state high court specifically identified at least four features that are common to many recognized special relationships:

1. Dependency: “Generally, the relationship has an aspect of dependency in which one party relies to some degree on the other for protection.” *Id.* at 620.
2. Control: “Whereas one party is dependent, the other has superior control over the means of protection.” *Id.* at 621.

1 3. Limited Communities: “[Special relationships] create a duty of care owed to a limited
2 community, not the public at large.” *Id.*

3 4. Beneficial to the duty-holder: “[A]lthough relationships often have advantages for both
4 participants, many special relationships especially benefit the party charged with a duty
5 of care.” *Id.* at 621.

6 The relationship here between Plaintiffs and Accellion exhibits all four features identified
7 in *Regents*. First, Plaintiffs have demonstrated that they relied on Accellion to safeguard the PII
8 that it transferred. The Complaint alleges that “[i]n the ordinary course of doing business with
9 entities that use Accellion’s FTA, individuals are typically *required to provide PII* that is then
10 *transferred by Accellion*,” and “when electronic files containing such information are transferred,
11 the transfer *must be secure*.” Compl. ¶¶ 30–31 (emphasis added). This reliance is all the more
12 heightened by the high value of PII and its frequent targeting by hackers and cybercriminals.
13 Compl. ¶¶ 63–64. Conversely, there is no reason to believe that Plaintiffs could have secured their
14 PII themselves when it was sent using Accellion’s FTA software.

15 Second, Plaintiffs have also alleged that Accellion has “superior control over the means of
16 protection.” *Regents*, 4 Cal. 5th at 621. The Complaint directly alleges that Accellion was “in the
17 position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to
18 Plaintiffs and Class members from a resulting data breach.” Compl. ¶ 120; *see also id.* ¶ 140.
19 Indeed, Accellion demonstrated this control when it released patches for the vulnerabilities within
20 days after they were exploited. Compl. ¶¶ 43, 46.

21 Third, consistent with *Regents*, this “relationship is limited to specific individuals” and
22 does not run to “the public at large.” 4 Cal. 5th at 621. As defined by the Complaint, the special
23 relationship in this case extends to “the end users of the services Accellion and Flagstar provided
24 to their clients,” *i.e.*, “those to whom the data belonged.” Compl. ¶¶ 119–120. Accellion objects
25 that imposing a duty in this instance would “expose [software] manufacturers to unmanageable
26 litigation risk.” Mot. 8; *see also* 10/19/23 Hr’g Tr. 10:11–18 (“Plaintiffs are essentially alleging
27 that Accellion had a special relationship with the public at large [] because anyone’s data could be

1 stored or transferred on Accellion’s software.”). However, the fact that the special relationship
2 *could* extend to any particular person in the public does not mean that the relationship is *with* the
3 public at large. If so, the “classic examples” of special relationships recognized at common law—
4 *e.g.*, the common carrier-passenger and innkeeper-guest relationships—would fall out of this
5 definition, given that any member of the public can conceivably board a public bus or book a room
6 at an inn. *See Regents*, 4 Cal. 5th at 620. Here, the special relationship exists only between
7 Accellion and those specific individuals whose information the FTA software ferries.

8 Finally, the Complaint alleges that Accellion is a benefactor of this special relationship,
9 given that “[t]his business model proved successful for Accellion for many years.” Compl. ¶¶ 29,
10 31. Indeed, “Accellion’s entire business model was built on promising its clients that it provided a
11 platform to securely transfer files that contained sensitive data.” *Id.* ¶ 120. In much the same way
12 that “[r]etail stores or hotels could not successfully operate [] without visits from their customers
13 and guests,” *Regents*, 4 Cal. 5th at 621, Accellion could not successfully operate without the need
14 for secure transfers of Plaintiffs’ sensitive data. *See* Compl. ¶¶ 30–31. Accordingly, all four
15 *Regent* features the existence of a special relationship between Accellion and Plaintiffs.

16 The Court’s finding of a “special relationship” between data companies and the owners of
17 the data is also consistent with the holdings that many courts have reached prior to the framework
18 established by *Regents* and *USAT*. Specifically, there is abundant authority that California law
19 recognizes a duty on companies to take reasonable steps to protect all sensitive information it
20 obtains from individuals. *See, e.g., Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898,
21 915 (S.D. Cal. 2020) (finding “no support [] for [defendant’s] argument that no special
22 relationship exists between a company that possesses peoples’ personal and medical information
23 and those people”); *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *3 (N.D. Cal. Sept. 14,
24 2016) (“[T]he *Rowland* factors compel the conclusion [defendant] was duty-bound to take
25 reasonable steps to protect all personal identifying information it obtained from its employees,
26 including information pertaining to employees’ spouses and dependents.”); *In re Facebook, Inc.,*
27 *Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 799 (N.D. Cal. 2019) (“Facebook had a

responsibility to handle its users’ sensitive information with care.”); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) (finding that a Facebook user had “met his obligation to plausibly plead duty of care” against Facebook “in the handling of personal information”).

Accellion argues that they had no relationship at all with Plaintiffs, contending that it lacks contractual privity with Plaintiffs and played no role in how Plaintiffs’ information was provided or used by its clients. Mot. 6. *Regents*, however, did not identify “privity of contract” or “direct correspondence” as common features of special relationships, even though both features were evidently present in the college-student relationship in *Regents*. 4 Cal. 5th at 622. Moreover, federal courts applying California law have not hesitated to extend a data company’s duty of care beyond those with whom it shares privity or exceeds some threshold level of interactions. *See Stasi*, 501 F. Supp. 3d at 915 (finding that defendant healthcare software company “owed a duty to protect Plaintiffs’ information despite the fact that Plaintiffs were not [defendant’s] customers or otherwise in privity with [defendant]”); *Castillo*, 2016 WL 9280242, at *3 (finding that defendant was “duty-bound to take reasonable steps to protect all personal identifying information it obtained from its employees, *including information pertaining to employees’ spouses and dependents.*”) (emphasis added).

Accellion correctly point out that many of the decisions Plaintiffs rely on were decided prior to the California Supreme Court’s clarification of the “duty to protect” in *USAT*. Reply 3 n.2, 4. On the other hand, however, Accellion also has not cited any California law authority—either before or after *USAT*—to support its proposition that no “special relationship” exists between a data transfer company and the owners of the data being transferred. *See Stasi*, 501 F. Supp. 3d at 914 (finding there to be “no support, however, for [defendant’s] argument that no special relationship exists between a company that possesses peoples’ personal and medical information and those people”). In any event, the Court’s standalone “special relationship” analysis above comports with the *USAT* framework.

Accellion also relies heavily on *Doe v. Uber Techs., Inc.*, 79 Cal. App. 5th 410 (2022), for the proposition that a general public statement advertising “safe pickups” for customers did not

create a special relationship between Uber and the victim plaintiffs. Mot. 6–7. However, the California Court of Appeal’s analysis in *Uber* did not turn on the type of special relationship in this case (*i.e.*, between a file transfer company and the owners of the information it shared). Rather, *Uber* only analyzed whether a special relationship existed based upon on a “common carrier-passenger” basis and on a contractual basis. 79 Cal. App. 5th at 420–24. Accordingly, *Uber*’s “special relationship” analysis provides limited insight into whether a special relationship exists between a file transfer software company and the owners of the data.

In sum, the Court finds that Plaintiffs have alleged the existence of a special relationship between themselves and Defendant Accellion, satisfying the first step of *USAT*’s two-step inquiry for duties to protect.

b. Rowland Factors

The Court turns next to consider whether any of the factors identified in *Rowland v. Christian*, 69 Cal. 2d 108 (1968), would limit the duty that Accellion owed on account of this special relationship. *See USAT*, 11 Cal. 5th at 209. These factors include: “the foreseeability of harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant’s conduct and the injury suffered, the moral blame attached to the defendant’s conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and the availability, cost, and prevalence of insurance for the risk involved.” *Rowland*, 69 Cal. 2d at 113.

The Court finds that the Complaint’s allegations track these factors and plead appropriate and specific facts regarding the foreseeability of harm from Accellion’s conduct, Plaintiffs’ injuries, the nexus between Accellion’s failure to employ reasonable security protections and Plaintiffs’ injuries, and the policy of preventing future harm. Compl. ¶¶ 137–141. The only factor advanced by Accellion to limit the duty is the public policy argument that “[p]ermitting the customers of a software company’s customers to sue the company directly would negate its ability to contractually manage its own risk, by exposing it to limitless and unforeseeable liability.”

Reply 3 (emphasis in original). At the hearing, Accellion analogized this duty to Microsoft Outlook or Amazon Web Services owing a duty to anyone whose information passes through their services. 10/19/23 Hr’g Tr. 5:5–16. Accellion, however, does not explain how this policy would narrow the duty imposed. Additionally, the only support cited for this policy argument is a 1986 U.S. Supreme Court opinion standing for the general proposition that it would be “difficult for a manufacturer to take into account the expectations of persons downstream who may encounter its product,” which is too thin a reed and too general a premise for the Court to accord meaningful weight. Reply 3–4 (citing *E. River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858 (1986)). Accellion also does not make any effort to reconcile this public policy with existing statutory duties. Indeed, as noted in *Stasi*, “the burden of imposing a common law duty to protect [] personal information is not likely high given that both state and federal law already require such protection, and, in the case of state law, already allows for a private right of action.” 501 F. Supp. 3d at 915. In any event, courts analyzing duties to protect data under *Rowland* have typically found that, “[f]rom a policy standpoint, to hold that [the company] has no duty of care here ‘would create perverse incentives for businesses who profit off the use of consumers’ personal data to turn a blind eye and ignore known security risks.’” *Bass*, 394 F. Supp. 3d at 1039 (citing *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019)).

It is also worth reiterating that, prior to the 2021 decision in *Brown v. USAT*, California courts were using the *Rowland* factors to find that data companies owed duties of care in handling the personal information they received. *See, e.g., Bass*, 394 F. Supp. 3d 1039 (finding a duty of “reasonable care in the handling of personal information” after analyzing *Rowland* factors); *Stasi*, 501 F. Supp. 3d 915 (“Applied here, [the *Rowland*] factors weigh in favor of the plausibility that [defendant] owed a duty to protect Plaintiffs’ information despite the fact that Plaintiffs were not [defendant’s] customers or otherwise in privity with [defendant].”); *Castillo*, 2016 WL 9280242, at *3 (“[T]he *Rowland* factors compel the conclusion [defendant] was duty-bound to take reasonable steps to protect all personal identifying information it obtained from its employees, including information pertaining to employees’ spouses and dependents.”).

Given the Complaint’s allegations and the overall weight of *Rowland* analyses in data protection cases, the Court finds that the *Rowland* factors do not warrant any further limitation of the duty imposed by the “special relationship” found above.

* * *

In summary, the Court finds that Plaintiffs have alleged that there exists a “special relationship” between Accellion and the Plaintiffs who own the PII that Accellion handled, giving rise to a duty of reasonable care to protect Plaintiffs’ PII.

2. Breach

The Complaint alleges that Accellion breached its duties by failing to (1) adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and Class members’ PII; (2) adequately monitor the security of its networks and systems; (3) provide timely notice that Plaintiffs and Class members’ PII had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and (4) ensure that clients were timely notified about the FTA security vulnerabilities. Compl. ¶¶ 133–34. The Complaint also incorporates by reference a March 2021 security assessment report issued by the cybersecurity firm Mandiant (“Mandiant Report”), which found that the two vulnerabilities exploited during the data breaches were of “critical severity.” Compl. ¶ 48 n.13. In addition to those “critical” vulnerabilities, the Mandiant Report also identified two other vulnerabilities that were of “high severity” and “medium severity.” *Id.*

As a preliminary matter, there is some support for the proposition that, where a data breach has occurred, the breach itself is sufficient to allege a breach of duty for Rule 12(b)(6) purposes. In *Flores-Mendez v. Zoosk, Inc.*, Judge Alsup invoked the common law doctrine of *res ipsa loquitur* (“the thing speaks for itself”) to hold, “when a breach occurs, *the thing speaks for itself*. The breach would not have occurred but for inadequate security measures, or so it can be reasonably inferred at the pleadings stage.” 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021). This reasoning was motivated in part by Judge Alsup’s observation that, in data breach cases, it would be “unreasonable for defendant to insist that the details be laid out in the initial complaint,”

1 because the “ordinary consumer [] has no clue what internet companies’ security steps are.” *Id.*
2 The Court agrees that this reasoning has some currency, though it need not fully embrace the
3 analysis here, given that Plaintiffs *have* alleged deficiencies in Accellion’s security measures.

4 In this case, the Court finds that the findings published in the Mandiant Report and
5 incorporated by reference into the Complaint are sufficient to allege breach for negligence
6 purposes. Neither party attempts to assail Mandiant’s reputability, and both parties have agreed
7 the Court may place great reliance on the Report’s findings. 10/19/23 Hr’g Tr. 17:23–18:2, 25:1–
8 12. To that end, the Court finds that the Mandiant Report provides great detail into the
9 vulnerabilities exploited by the two data breaches in this case, which included SQL injection,
10 server-side request forgery, and remote command execution. Mandiant Report 6–7. The
11 existences of these “critical severity” vulnerabilities, in addition to two other “high” and
12 “medium” level vulnerabilities, are sufficient for Plaintiffs to plausibly allege that Accellion
13 breached its duty of reasonable care to protect their PII. These vulnerabilities and breach
14 allegations do not turn on the allegations that Accellion failed to retire the FTA product as it
15 neared its end-of-life, contrary to Accellion’s suggestion. Reply 8–9.

16 Accordingly, the Court finds that the Complaint has sufficiently plead breach with regards
17 to Plaintiffs’ negligence claim.

18 **3. Damages**

19 “Under California law, appreciable, nonspeculative, present harm is an essential element of
20 a negligence cause of action.” *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 649 (N.D. Cal. 2020).

21 With respect to damages, the Complaint alleges that Plaintiffs have experienced the loss of
22 their ability to control how their personal information is used; increased risk of future identity
23 theft; costs associated with credit and asset freezes due to credit misuse; out-of-pocket expenses
24 associated with preventing, detecting, and recovering from identity theft; and diminution in value
25 of their personal information. Compl. ¶ 143.

26 Accellion argues that these injuries are not cognizable and also that the economic loss rule
27 bars Plaintiffs’ recovery. Mot. 9–11. The Court addresses each in turn.

28 Case No.: [5:21-cv-01155-EJD](#)

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

With respect to Accellion’s first argument, the Court finds that the Complaint has sufficiently alleged injury for Plaintiffs’ negligence claim. Plaintiffs here have already experienced identity theft in the form of unauthorized charges appearing on their bank and credit accounts, Compl. ¶¶ 5–15, rendering the risk of future identity theft sufficiently non-speculative. Additionally, a “growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory. And a growing number of courts now recognize that individuals may be able to recover Consequential Out of Pocket Expenses that are incurred because of a data breach, including for time spent reviewing one’s credit accounts.” *In re Experian Data Breach Litig.*, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016) (internal brackets and quotation marks omitted). Courts have also recognized “time spent responding to a data breach” as a non-economic injury. *Stasi*, 501 F. Supp. 3d at 913. These are all cognizable categories of damages for a negligence cause of action under California law.

Turning next to Accellion’s argument as to the economic loss rule, the Court also finds that the injuries alleged in the Complaint constitutes non-economic injuries that do not implicate the economic loss rule. For instance, “time spent responding to a data breach is a non-economic injury, that when alleged to support a negligence claim, defeats an economic loss doctrine argument.” *Stasi*, 501 F. Supp. 3d at 913 (citing *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1295 (S.D. Cal. 2020); *see also Schmitt v. SN Servicing Corp.*, 2021 WL 3493754, at *6 (N.D. Cal. Aug. 9, 2021) (collecting cases in this district that “have found that the economic loss doctrine does not apply where loss of time is alleged”). Additionally, California law carves out an exception to the economic loss rule where a “special relationship” exists between the parties, which the Court has already found the Complaint to have alleged. *See supra* Section III(A)(1)(a); *J’Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979) (“Where a special relationship exists between the parties, a plaintiff may recover for loss of expected economic advantage through the negligent performance of a contract although the parties were not in contractual privity.”). Each of these bases is an independent reason that prevents Plaintiffs’ negligence claim from being dismissed under the economic loss rule.

At the hearing (but not in its briefs), Accellion emphatically commended the 1965 California Supreme Court decision of *Seely v. White Motor Co.*, 63 Cal. 2d 9 (1965), to the Court in support of its economic loss rule argument. However, *Seely* is not the panacea Accellion presents it as. *Seely* was a warranty case relating to defendant manufacturer’s failure to repair plaintiff’s truck and did *not* involve a negligence claim for tort recovery. 63 Cal. 2d at 13 (affirming judgment against defendant because the “award was proper on the basis of a *breach of express warranty*”) (emphasis added). Moreover, *Seely* did not analyze whether a “special relationship” exists between a truck manufacturer and the truck end user—it primarily engaged in a discourse regarding the differences between tort and warranty liability. *Id.* at 15–19. To the extent that Accellion relies on *Seely*’s singular statement that, “[e]ven in actions for negligence, a manufacturer’s liability is limited to damages for physical injuries and there is no recovery for economic loss alone, *id.* at 18, this merely restates the general economic loss rule. Contrary to Accellion’s insistence, this does *not* bear upon the question of whether a manufacturer has a “special relationship” to downstream persons affected by the product. *See* 10/19/23 Hr’g Tr. 43:1–17. Notwithstanding Justice Traynor’s well-reasoned decision, the duties, alleged injuries, and relationship between the *Seely* parties bear little resemblance or application to the case at bar, which involves the relationship between a file transfer software company and the individuals whose PII was compromised relating to a data breach.

Accordingly, the Court finds that Plaintiffs have sufficiently alleged damages for their negligence claim that are cognizable and not barred by the economic loss rule.

* * *

Because the Court finds that a special relationship exists between the parties that give rise to a duty of care, that Accellion breached its duty, and Plaintiffs have alleged cognizable damages, the Court DENIES Accellion’s motion to dismiss Plaintiffs’ First Claim for negligence.

B. Negligence Per Se

Accellion also moves to dismiss the Complaint’s second claim, which Plaintiffs style as “negligence per se.” Mot. 11. This claim alleges that Accellion’s conduct breached the duty

imposed under various statutory regimes, including the FTC Act, HIPAA, the California Customer Records Act (“CCRA”), and the Children’s Online Privacy Protection Act (“COPPA”).

Compl. ¶ 145. Accellion contends that this claim is improper because “negligence per se” is not an independent claim for relief under California law and, even properly wielded as an evidentiary doctrine, Plaintiffs may not rely on the specific statutes to establish a standard of care. Mot. 11.

Under California law, a “claim” for negligence per se requires four showings: “(1) a defendant violated a statute, ordinance, or regulation; (2) the violation proximately caused injury; (3) the injury resulted from an occurrence that the enactment of the law was designed to prevent; and (4) the plaintiff was a member of the class of persons the statute was intended to protect.” *Kirsten v. California Pizza Kitchen, Inc.*, 2022 WL 16894503, at *8 (C.D. Cal. July 29, 2022) (citing *Safari Club Int’l v. Rudolph*, 862 F. 3d 1113, 1126 (9th Cir. 2017)). “If all four requirements are satisfied, the plaintiff is entitled to a presumption that the defendant failed to exercise due care; however, the plaintiff still must plead an underlying negligence claim for which the presumption is to apply.” *Kilmer v. Medtronic, Inc.*, 2021 WL 1405198, at *7 n.5 (E.D. Cal. Apr. 13, 2021).

The Court agrees with Accellion to the extent that Plaintiffs may not maintain “negligence per se” as a standalone claim alongside their negligence claim, which Plaintiffs themselves do not appear to contest. Opp. 13 (recognizing that negligence per se is “not an independent cause of action”); *see, e.g., Jones v. Awad*, 39 Cal. App. 5th 1200, 1210 (2019) (“Negligence per se is an evidentiary doctrine, rather than an independent cause of action.”). On this point, the Court finds that the Complaint does not state an independent claim for relief labeled “negligence per se,” which is therefore subject to dismissal as a matter of law.

Accellion’s secondary arguments—that Plaintiffs have failed to allege why they may use the statutory standards of care to establish their negligence claim—are less persuasive. First, Accellion contends that the Complaint has not alleged proximate injury to property. Mot. 11. This argument is unavailing given that, as highlighted above at Section III.A.3, the Complaint has alleged a wide variety of injuries Plaintiffs have sustained from the data breaches. Second,

Accellion submits that plaintiffs may only rely on a statute’s duty if the statute in question prescribed a “particular course of conduct,” citing *Ramirez v. Nelson*, 44 Cal. 4th 908, 919 (2008). *Ramirez*, however, does not require that the statute lay out specific conduct before it can be referenced under negligence per se. Rather, the Supreme Court of California’s holding turned on a nexus requirement between the transgressed statute and the injury sustained by the plaintiff asserting negligence per se. *Id.* at 918 (2008) (“[I]f one is not within the protected class or the injury did not result from an occurrence of the nature which the transgressed statute was designed to prevent, [negligence per se] has no application.”); *see also Jones*, 39 Cal. App. 5th at 1210 (“[Negligence per se] can be applied generally to establish a breach of due care under *any* negligence-related cause of action.”) (emphasis added).

Federal courts applying California law on negligence per se in data breach case have also turned to FTC Act and HIPAA provisions to supply the standard of care element for a standalone negligence claim. *See, e.g., Kirsten*, 2022 WL 16894503, at *9 (allowing reference to FTC Act Section 5 for “unfair . . . practices in or affecting commerce”); *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1142 (C.D. Cal. 2021) (allowing reference to FTC Act and HIPAA for breach of medical information). Here, although the Court does not find that Plaintiffs can maintain their negligence per se claim as a standalone cause of action, the Court also will not preclude Plaintiffs from relying on the provisions of the FTC Act, HIPAA, CCRA, or COPPA in support of the elements in their negligence claim, provided they can also meet the other requirements for negligence per se noted above.

Accordingly, the Court GRANTS Accellion’s motion and DISMISSES WITHOUT LEAVE TO AMEND the Complaint’s second claim for negligence per se. This dismissal, however, shall be WITHOUT PREJUDICE to Plaintiffs’ alleging the underlying statutes under their negligence claim to establish the applicable standards and duties of care.

C. California Consumer Privacy Act (“CCPA”)

Accellion moves to the dismiss Plaintiffs’ CCPA claim on two grounds: (1) Accellion is not a “business” within the meaning of the statute; and (2) the Complaint does not allege a specific

non-conclusory failure to implement reasonable security measures. Mot. 14. Because Accellion is not a “business” under the CCPA, the Court need not and will not address Accellion’s arguments as to its reasonable security measures.

The CCPA provides a limited civil cause of action for “[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of *the business’s violation* of the duty to implement and maintain reasonable security procedures.” Cal. Civ. Code § 1798.150(a)(1) (emphasis added). The CCPA defines “business,” in relevant part², as follows:

[A] legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that **collects consumers’ personal information**, or on the behalf of which such information is collected and that alone, or jointly with others, **determines the purposes and means of the processing of consumers’ personal information**. . . .

Id. § 1798.140(d)(1) (emphasis added). Accordingly, to qualify as a “business” under the CCPA, the entity must both (1) collect PII and (2) determine why and how (“the purposes and means”) the PII should be processed. *See Karter v. Epiq Sys., Inc.*, 2021 WL 4353274, at *2 (C.D. Cal. July 16, 2021). The CCPA further defines “collects” as “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means”; and defines “processing” as “any operation or set of operations that are performed on personal information or on sets of personal information.” Cal. Civ. Code § 1798.140(f), (y).

As to the first requirement, the Complaint contains several allegations of Accellion collecting consumers’ PII. *See, e.g.*, Compl. ¶¶ 2 (“Entities . . . hired Accellion—a cloud solutions company—to collect and securely transfer sensitive Personally Identifiable Information.”), 158 (“Defendants collect personal information from, among other sources, consumers who request information from them, consumers who use their services, including users of their mobile applications, and consumers who submit customer support requests.”). The CCPA also adopts a broad understanding of “collects,” defining it to mean “buying, renting, gathering, obtaining,

² Accellion does not dispute the other threshold revenue requirements set forth at Cal. Civ. Code § 1798.140(d)(A)–(C).

1 *receiving, or accessing any personal information pertaining to a consumer by any means.”*

2 Cal. Civ. Code § 1798.140(f) (emphasis added). On a Rule 12(b)(6) motion, the Complaint’s
3 allegations are sufficient (though barely) to state that Accellion “collects consumers’ personal
4 information” under the CCPA’s broad definition.

5 The second half of the “business” definition, however, entails a more nuanced analysis.
6 The Complaint alleges that Accellion was hired by various companies to “securely transfer” and to
7 “facilitate secure, encrypted file sharing that exceeded limits imposed on the size of emails
8 attachments.” Compl. ¶¶ 2, 25 (“Instead of transferring documents by email, the intended
9 recipient would receive a link to files, hosted on Accellion’s FTA, which could then be viewed or
10 downloaded.”). Therefore, the relevant inquiry is whether, by enabling the secure transfer of files
11 by hosting them on FTA, Accellion determined why and how consumers’ PII was processed.

12 So alleged, the Court finds that Accellion did not. Critically, the Complaint lacks any
13 allegations regarding the “determinations” Accellion made with respect to why and how Plaintiffs’
14 PII was processed. The allegation that Accellion “developed, marketed, and sold a file sharing
15 transfer software product” (Compl. ¶ 25) does not indicate that Accellion would be making
16 decisions about the data its software would transfer after the software was licensed or made
17 available to a customer. Nor does the Complaint allege that Accellion decides or “determines”
18 anything about PII processing whenever one of its customers uses the FTA product to send files.
19 To the contrary, the Complaint contains statements indicating that it is Accellion’s *customer* who
20 makes the decision for each file transfer. Compl. ¶¶ 2, 28 (alleging that Accellion “*enables*
21 *millions. . . from every walk of life to do their jobs* without putting *their organization* at risk.
22 *When they click the Accellion button, they know it’s the safe and secure way to share information*
23 *with the outside world*”) (emphasis added). The relevant CCPA inquiry is not whether Accellion
24 simply enabled or was involved in transmitting Plaintiffs’ PII; rather, the Court must ask whether
25 Accellion *determined* how and why Plaintiffs’ PII was transmitted. Without any allegations as to
26 what Accellion decides or “determines” with respect to processing Plaintiffs’ PII, the Court cannot
27 find that the Complaint has alleged that Accellion is a “business” for the purposes of the CCPA.

28 Case No.: [5:21-cv-01155-EJD](#)

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Accellion’s involvement (or lack thereof) with respect to determining how a consumers’ PII is processed also distinguishes it from other companies that courts have found to be “businesses” under the CCPA. In *Karter v. Epiq Systems, Inc.*, the complaint had specifically alleged that the defendant (a class action settlement administrator) “work[ed] with its clients to determine how it will use consumers’ personal information to provide notice and manage claims and opt-outs.” 2021 WL 4353274, at *2 (C.D. Cal. July 16, 2021). Unlike Accellion, the *Epiq* defendant was alleged to have directly and affirmatively participated in determining how a consumer’s PII would be used. Similarly, in *Blackbaud*, the court found that a company that provided software for “administration, fundraising, marketing, and analytics to social good entities” was a “business” under the CCPA. *In re Blackbaud, Inc., Customer Data Breach Litig.*, 2021 WL 3568394 (D.S.C. Aug. 12, 2021). There as well, the defendant was alleged to have actively interacted with and analyzed the data at issue: “Blackbaud *uses consumers’ personal data* to provide services at customers’ requests, as well as *to develop, improve, and test Blackbaud’s services*,” that “Blackbaud develops software solutions to process its customers’ patrons’ personal information,” and that “Blackbaud offers ‘professional and managed services in which its expert consultants provide *data conversion, implementation, and customization services* for each of its software solutions.’” *Id.* at *5 (emphasis added). In both *Epiq* and *Blackbaud*, the defendants played much more integral roles in determining how to process consumer PII—they were involved in, analyzed, and even consulted on how consumers’ personal information would be used. Accellion did not.

Plaintiffs argue that “[b]y facilitating the transfer of personal information, Accellion enabled the use of consumers’ PII and determined the means of processing it.” Opp. 15. At oral arguments, Plaintiffs’ counsel expanded on this argument, submitting that the “purpose” of the FTA product was to “put files up on the cloud and transfer them” and the “means is just the proprietary technology.” 10/19/23 Hr’g Tr. 36:10–24. This, however, conflates the “purposes and means” of the *FTA software* with the “purposes and means of the *processing of consumers’ personal information*,” a construction that is not supported by the CCPA or the Complaint. The

CCPA specifically defines “processing” as “any operation or set of operations that are performed on personal information or on sets of personal information.”³ Cal. Civ. Code § 1798.140(y) (emphasis added). The Complaint, however, does not allege that the FTA software performs any operation on the information that it transfers, only that it “facilitate[s] secure, encrypted file sharing.” Compl. ¶ 25. Accordingly, the Court will decline Plaintiffs’ invitation to find that Accellion “determine[d] the purposes and means of the processing of consumers’ personal information” by simply developing and marketing a file sharing software.

Additionally, Plaintiffs rely on statements Accellion made in its privacy policy that it controls information provided directly to it. Compl. ¶ 28. However, the information referenced by this privacy policy appears to relate only to Accellion’s interactions with its direct clients (*e.g.*, Flagstar), as opposed to information transmitted between Accellion’s clients and the Plaintiffs. *See Accellion Privacy Policy*, Kiteworks, <https://www.kiteworks.com/privacy-policy/> (“We respectfully use appropriate personal information in order to *market, sell, deliver, and support the solutions that we offer*. We do not collect personal information that is not necessary for the marketing, selling, delivery, and support of our solutions, such as demographic, biometric, medical, social information. . . . Our systems, employees, contractors, and affiliates *can not access personal information collected by our customers* even when that information may be contained in customer applications which use the Accellion Services under the control of customers.”). Plaintiffs contend that the CCPA does not require that the information involved in a breach be the same type of information a business collects or processes. Opp. 15–16. However, even if Accellion may be a “business” with respect to data it collects from its website, the CCPA expressly provides that the duty of “reasonable security procedures and practices” imposed on businesses only runs to the personal information that the business collects. Cal. Civ. Code §

³ Notably, the CCPA did *not* include “sharing” or “transferring” personal information within the definition for “processing,” even though the statute evidently contemplated sharing consumers’ personal information. *See* Cal. Civ. Code § 1798.140 (ah)(1) (defining “sharing” as “sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party”).

1798.100(e). On that point, the Complaint asserts no CCPA claim against the security measures protecting the personal information collected pursuant to Accellion’s privacy policy.

Because the Complaint fails to allege that Accellion is a “business” under the CCPA with respect to Plaintiffs’ PII, Plaintiffs cannot maintain their CCPA claim against Accellion, and the Court need not address Accellion’s other CCPA arguments. Accellion’s motion to dismiss the CCPA claim is GRANTED. Because the Court cannot conclude that Plaintiffs would be unable to resolve these deficiencies with further factual amendment regarding the FTA product’s operation on their PII, the Third Claim is DISMISSED WITH LEAVE TO AMEND.

D. Confidentiality of Medical Information Act (“CMIA”)

Plaintiffs also allege that Accellion violated its obligations under the expanded CMIA definitions for businesses deemed to be a “provider of health care.” Specifically, the Complaint alleges that, under Cal. Civ. Code § 56.06(a), Accellion is “organized in part for the purpose of maintaining medical information to make it available . . . for purposes of information management, diagnosis, or treatment.” Compl. ¶ 167; *see also* Cal. Civ. Code § 56.06(a). The Complaint also alleges that Accellion falls under the definition at § 56.06(b) as a business offering “software that is designed to maintain medical information.” Compl. ¶ 167; *see also* Cal. Civ. Code § 56.06(b).

Accellion argues that the CMIA claim is deficient because (1) Accellion is not an entity regulated by the CMIA; (2) Plaintiffs fail to allege that their medical information was affected by the data breaches; and (3) Plaintiffs failed to allege negligence. Mot. 15–17.

The Court agrees with Accellion that it does not fall within the expanded § 56.06 definitions of a “provider of health care.” First, under § 56.06(a), Plaintiffs have failed to sufficiently allege that Accellion is a “business organized for the purpose of maintaining medical information.” Cal. Civ. Code § 56.06(a). In their opposition, Plaintiffs refer to their allegation at ¶ 167 that “Accellion is organized in part for the purpose of maintaining medical information” (Opp. 18); however, conclusory recitations of the requisite statutory showing are not enough to state a claim. *See, e.g., Iqbal*, 556 U.S. at 678. The only non-conclusory allegation in the

Complaint states that Accellion “provides secure file-sharing services for hospitals and other medical professionals to facilitate ‘patient care’ through the sharing of patient’s medical records.” Compl. ¶ 167. However, § 56.06(a) requires more than an allegation that Accellion maintained or even presently maintains medical information; Accellion must have been “organized *for the purpose of* maintaining medical information.” Here, the Court cannot infer from a single website statement advertising its breadth of clients that Accellion is a company organized for the purpose of maintaining medical information.

Second, under § 56.06(b), the Court also finds that Plaintiffs have failed to allege that Accellion is a business that offered “software or hardware to consumers . . . that is designed to maintain medical information.” As a preliminary matter, both parties appear to agree that Accellion’s software was not offered directly to individual consumers. *See* Mot. 16; Opp. 17–18. However, Plaintiffs contend that Accellion nonetheless falls within this category because its institutional customers (*e.g.*, “government agencies, private business, and universities,” Compl. ¶ 2) should also be considered “consumers” as purchasers of Accellion’s software. *See* Opp. 19 (citing *Blackbaud*, 2021 WL 3568394, at *7 (interpreting “consumers” as encompassing more than just “individuals”).

This is a tenuous interpretation that threatens to read the “consumers” language out of the statute. Plaintiffs’ overly generalized definition of a consumer as “one that utilizes economic goods” would be redundant and duplicative with the immediately preceding language referring to a “business that *offers* software or hardware to consumers.” Cal. Civ. Code § 56.06(b). Who else would a business “offer” software to, if not “one that utilizes” the software? Additionally, Plaintiffs’ expansion of “consumers” to include business entities would be inconsistent with the CMIA’s usage of “consumers” in other contexts, which often concern the consumer’s “diagnosed mental health or substance use disorder” or “mental health application information” collected from a consumer. *See* Cal. Civ. Code § 56.05(j), (k). Accordingly, the Court declines to adopt Plaintiffs’ and *Blackbaud*’s interpretation of “consumers” as “one that utilizes economic goods.” Additionally, the Court also finds that Accellion would not fall under the § 56.06(b) category for

the separate reason that its FTA software was not “designed to maintain medical information.” Much like the analysis under § 56.06(a), the fact that the FTA may have been used to transfer or maintain medical information does not mean it was *designed* to do so.

At the hearing, Plaintiffs directed the Court to *Prutsmann v. Nonstop Admin. & Ins. Servs., Inc.*, 2023 WL 5257696 (N.D. Cal. Aug. 16, 2023) in support of their overall position.⁴ Although *Prutsmann* declined to dismiss the CMIA claim, the parties there did not dispute whether the defendant or its software was intended to “maintain medical information”; indeed, the defendant had admitted that it was an “employee health insurance and benefits broker” that provided “healthcare insurance solutions.” Consolidated Am. Compl. ¶¶ 48–49, *Prutsmann v. Nonstop Admin. & Ins. Servs., Inc.*, No. 23-CV-01131-VC (N.D. Cal. May 25, 2023), ECF No. 38. This case, therefore, offers limited persuasive weight here. Accellion and its file transfer software are much farther removed from medical information than a health insurance broker would be.

Because the Complaint lacks facts from which the Court could reasonably infer that Accellion was “organized for the purpose of maintaining medical information” or offered software to consumers that is “designed to maintain medical information,” Plaintiffs have failed to allege that Accellion is subject to CMIA obligations. Although the Court believes it unlikely that Plaintiffs could discover and allege facts indicating that Accellion was designed to “maintain medical information,” the Court cannot conclude that it would be futile. Accordingly, the Court GRANTS Accellion’s motion and DISMISSES the CMIA claim WITH LEAVE TO AMEND.

E. California Customer Records Act (“CCRA”)

The Complaint asserts a CCRA claim against Accellion, alleging that Accellion’s failure to promptly notify Plaintiffs violated its obligations under the CCRA. Compl. ¶¶ 183–84. Accellion moves to dismiss this claim, arguing that (1) Plaintiffs are not Accellion’s “customers” and therefore may not initiate a civil action against it; (2) any obligation to notify Plaintiffs belonged

⁴ Plaintiffs originally cited *Prutsmann* in support of their CCPA claim. 10/19/23 Hr’g Tr. 40:20–24. However, *Prutsmann* only committed two sentences to discussing whether the defendant was a “business” under the CCPA without any analysis for the Court to follow.

to Accellion’s FTA customers, not Accellion; and (3) Plaintiffs’ allegations of actions they *could have taken* with timely disclosure are not cognizable injuries under the CCRA. Mot. 17–19.

The CCRA limits civil actions to “any *customer* injured by a violation of this title,” Cal. Civ. Code § 1798.84(b), which is defined as “an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.” *Id.* § 1798.80(c).

The Complaint alleges that Plaintiffs “provided personal information to Defendants for the purpose of obtaining services from Defendants” and, therefore, fall within the CCRA’s definition of “customer.” Compl. ¶ 179. Although this conclusion may be supported with respect to Accellion’s clients such as Flagstar Bank, it is not supported as to Accellion to the extent that Plaintiffs had sought to obtain services from—*i.e.*, were customers of—Accellion. The Complaint’s allegations indicate that Plaintiffs are customers or employees of Flagstar (*id.* ¶¶ 5, 8, 10), employees or customers of Kroger (*id.* ¶¶ 6, 7, 13, 14), recipients of health care services (*id.* ¶¶ 9, 12), or recipients of Washington unemployment benefits (*id.* ¶¶ 11, 15). There are no allegations that Plaintiffs had paid money to or obtained any service from Defendant Accellion.

Plaintiffs contend that “individuals do not have to provide their information directly to a business to be ‘customers’ under the CCRA.” Opp. 20–21. Even if the Court accepts this base proposition,⁵ Plaintiffs do not address the express requirement in the CCRA that the information be provided “for the purpose of . . . obtaining a service from the business.” Cal. Civ. Code § 1798.80(c). The Complaint contains no allegation that Plaintiffs intended to obtain any services from Accellion. Plaintiffs’ interpretation of “customers” under the CCRA is untenable given the unambiguous language in the statute.

Because Plaintiffs are not “customers” of Accellion within the meaning of the CCRA, the

⁵ To be clear, even this contention is on uncertain footing. Plaintiffs rely on a 2016 opinion that has been described more recently as an “outlier among courts considering this question [of whether the CCRA applies to non-customer information].” *Kirsten v. California Pizza Kitchen, Inc.*, 2022 WL 16894503, at *6 (C.D. Cal. July 29, 2022) (referring to *Castillo*, 2016 WL 9280242, at *7).

Court finds that they may not maintain their CCRA claim against Accellion. Accellion’s motion is GRANTED. Although the Court is not persuaded by Plaintiffs’ interpretation of the CCRA, it cannot conclude that Plaintiffs cannot plead facts that bring themselves within the definition of a “customer” and, therefore, the CCRA claim is DISMISSED WITH LEAVE TO AMEND.

F. Privacy Claims

Plaintiffs also bring two privacy claims against Accellion: the intentional tort of intrusion upon seclusion (Sixth Claim) and violation of the California Constitution’s right to privacy (Tenth Claim). Accellion moves to dismiss these claims on identical grounds, asserting that the Complaint contains no allegations of Accellion’s culpable state of mind for these intentional torts. Mot. 19–20. Plaintiffs respond that Accellion’s intent may be inferred from its “reckless disregard,” which purportedly suffices to establish intent for their privacy claims. Opp. 22.

“To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy,” and (2) the intrusion “occurred in a manner highly offensive to a reasonable person.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (internal brackets and quotation marks omitted) (citing *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 286 (2009)). A claim for invasion of privacy under the California constitution requires Plaintiffs to show: “(1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is ‘so serious . . . as to constitute an egregious breach of the social norms’ such that the breach is ‘highly offensive.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 601.

With respect to the intrusion upon seclusion claim, the Court finds that the Complaint has failed to allege that Accellion had acted intentionally with respect to the data breach. The Complaint only alleges that Accellion had “acted knowingly and in reckless disregard” of Plaintiffs’ privacy rights. Compl. ¶ 190. However, as courts in this district have found, there is “no authority that suggests that failure to take adequate measures to protect against the intentional intrusion of a third party satisfies the first element of a claim for intrusion on seclusion.” *Danner*

1 v. *Facebook Inc.*, 2020 WL 7862706, at *6 (N.D. Cal. Dec. 31, 2020). Plaintiffs cite Kentucky
2 and Nevada opinions for the proposition that “reckless disregard” is sufficient to establish intent
3 for an invasion of privacy claim. See Opp. 22 (citing *Smith v. Bob Smith Chevrolet, Inc.*, 275 F.
4 Supp. 2d 808 (W.D. Ky. 2003); *Dobson v. Sprint Nextel Corp.*, 2014 WL 553314 (D. Nev. Feb.
5 10, 2014)). However, both decisions only analyzed Kentucky and Nevada law, respectively, and
6 provide no insight into the proper applications of the California tort asserted here. Plaintiffs also
7 cite *Katsaris v. Cook*, 180 Cal. App. 3d 256 (1986), a 1986 California Court of Appeal decision to
8 describe how “reckless disregard” may be proven. *Katsaris* was a tort action for intentional
9 infliction of emotional distress (not intrusion upon seclusion) where the defendant had shot two of
10 plaintiff’s dogs—it shares no overlap with privacy torts or data breaches. *Id.* at 261. Plaintiffs’
11 Sixth Claim for intrusion upon seclusion may be dismissed on this ground alone.

12 As to Plaintiffs’ invasion of privacy claim under the California Constitution, the Court also
13 finds that Plaintiffs have not alleged that Accellion’s conduct was “highly offensive.” The
14 Complaint alleges that Accellion’s “fail[ure] to protect [personal] information from unauthorized
15 disclosure to third parties” was highly offensive. Compl. ¶¶ 189, 227. The weight of California
16 authority, however, cuts against this conclusory allegation. “[T]he highly offensive analysis
17 focuses on the degree to which the intrusion is unacceptable as a matter of public policy.” *In re*
18 *Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606. Notably, courts have declined to find
19 “highly offensive” conduct or an “egregious breach of social norms” where only negligence is
20 alleged with respect to a data breach, as opposed to intentional violations of privacy rights. See,
21 e.g., *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *12 (S.D. Cal.
22 Nov. 3, 2016) (dismissing invasion of privacy constitutional claim because “Plaintiff fails . . . to
23 allege any facts that would suggest that the data breach was an intentional violation of Plaintiff’s
24 and other class members’ privacy, as opposed to merely a negligent one”); *In re iPhone*
25 *Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (“Even negligent conduct that
26 leads to theft of highly personal information, including social security numbers, does not
27 ‘approach [the] standard’ of actionable conduct under the California Constitution and thus does

not constitute a violation of Plaintiffs’ right to privacy.”); *Ruiz v. Gap, Inc.*, 380 F. App’x 689, 693 (9th Cir. 2010) (noting that “California courts have yet to extend the [invasion of privacy] cause of action to include accidental or negligent conduct”); *cf. Prutsman*, 2023 WL 5257696 (dismissing claims for intrusion upon exclusion and California Constitution privacy rights because “[n]othing in the complaint suggests that Nonstop was anything but negligent and passive”). As a result, the Court does not find that Plaintiffs have alleged “highly offensive” conduct by Accellion, which is an element of both the intrusion upon seclusion and invasion of privacy claims.

Accordingly, because the Complaint has failed to allege that Accellion intentionally intruded or that the intrusion was *highly offensive*, Plaintiffs’ Sixth and Tenth Claims are DISMISSED WITH LEAVE TO AMEND.

G. Breach of Contract

Plaintiffs also brings a claim for breach of contract against Accellion as third-party beneficiaries. Compl. ¶ 198. Accellion moves to dismiss this claim because (1) it shares no privity of contract with any Plaintiff, and (2) the End User License Agreement (“EULA”) governing Accellion’s relationship with its clients contained an express clause disclaim any third-party beneficiaries.⁶ Mot. 20–21.

The Court agrees with Accellion that the third-party beneficiary disclaimer clause control in this case and preclude Plaintiffs from recovery as intended third-party beneficiaries. “For a third party to be able to recover on a contract, it must be able to show that the contract was made with the ‘express or implied intention of the parties to the contract to benefit the third party.’” *Dollar Tree Stores Inc. v. Toyama Partners LLC*, 2011 WL 872724, at *3 (N.D. Cal. Mar. 11, 2011). However, the Ninth Circuit has held that a “No Third Party Beneficiaries” clause “unambiguously manifests an intent not to create any obligations to third parties.” *Balsam v. Tucows Inc.*, 627 F.3d 1158, 1163 (9th Cir. 2010). Plaintiffs’ sole response—that the EULA disclaimer “serves only as evidence of the parties’ intent, and there is no factual record

⁶ The Court GRANTS Accellion’s request for judicial notice of the EULA, as Plaintiffs do not oppose taking notice. ECF No. 175; *see also* Opp. 23 n.8.

demonstrating intent,” Opp. 23—does not impair the unambiguous intent expressed in the EULA’s disclaimer language. In any event, their argument does not satisfy their pleading obligations as to whether Accellion or its clients intended Plaintiffs to be third-party beneficiaries.

Because the Court finds that Plaintiffs have not alleged privity of contract with Accellion nor have they alleged facts that would support an intent to create third-party beneficiary obligations, the Court GRANTS Accellion’s motion to dismiss the breach of contract claim WITHOUT LEAVE TO AMEND.

H. Unjust Enrichment

Accellion moves to dismiss Plaintiffs’ unjust enrichment claim, arguing that the Complaint does not sufficiently allege (1) inadequacy of legal remedies, or (2) the elements for unjust enrichment. Mot. 22–23.

The remedy for an unjust enrichment claim is equitable restitution. *Hartford Cas. Ins. Co. v. J.R. Mktg., L.L.C.*, 61 Cal. 4th 988, 998 (2015) (“An individual who has been unjustly enriched at the expense of another may be required to make restitution.”). Accordingly, Plaintiffs are required to allege that the Court has equitable jurisdiction over this claim, including a showing that they lack an adequate remedy at law. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020).

Here, the Complaint contains no allegations regarding the adequacy of Plaintiffs’ legal remedies. *See generally* Compl. ¶¶ 213–224. Plaintiffs respond that they have pled their unjust enrichment claim in the alternative to their claims at law, which they contend is sufficient to establish equitable jurisdiction. Opp. 24; *see also* Compl. ¶ 214. However, this response misses the mark. “The question is not whether or when Plaintiffs are required to choose between two available inconsistent remedies, it is whether equitable remedies are available to Plaintiffs at all,” specifically because of inadequate legal remedies. *In re MacBook Keyboard Litig.*, 2020 WL 6047253, at *2 (N.D. Cal. Oct. 13, 2020); *see also In re Apple Processor Litig.*, 2023 WL 5950622, at *2 (9th Cir. Sept. 13, 2023) (affirming dismissal under *Sonner* where “Plaintiffs were obligated to allege that they had no adequate legal remedy in order to state a claim for equitable

relief, and they have ‘fail[ed] to explain’ how the money they seek through restitution is any different than the money they seek as damages”). Likewise, the Court here finds that simply asserting their equitable claim in the alternative does not satisfy Plaintiffs’ burden to allege that they lack an adequate remedy at law.

Because Plaintiffs have failed to allege facts supporting the Court’s equitable jurisdiction, Plaintiffs’ Ninth Claim for unjust enrichment is DISMISSED WITH LEAVE TO AMEND.

I. Washington Consumer Protection Act (“WCPA”)

Finally, Accellion moves to dismiss the WCPA claim because Plaintiffs failed to allege an “unfair or deceptive act or practice” with respect to Accellion’s data security practices. Mot. 25. Accellion first argues that the Complaint does not allege specific security practices that it failed to implement (*id.*), and in its reply, Accellion argues that Plaintiffs cannot maintain a WCPA claim where the data breach impacted the customers of Accellion’s customers (Reply 12–13).

“[T]o prevail in a private [WCPA] action and therefore be entitled to attorney fees, a plaintiff must establish five distinct elements: (1) unfair or deceptive act or practice; (2) occurring in trade or commerce; (3) public interest impact; (4) injury to plaintiff in his or her business or property; (5) causation.” *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wash. 2d 778, 780 (1986). “Because the [WCPA] does not define ‘unfair or deceptive, the Washington Supreme Court has allowed the definitions to evolve through a gradual process of judicial inclusion and exclusion.” *Krefting v. Kaye-Smith Enterprises Inc.*, 2023 WL 4846850, at *8 (W.D. Wash. July 28, 2023). An “unfair act” is one that “(1) causes or is likely to cause substantial injury, which (2) consumers cannot avoid, and (3) is not ‘outweighed by countervailing benefits.’” *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1161 (W.D. Wash. 2017).

With respect to Accellion’s argument that the Complaint does not allege specific security measures it failed to maintain, the Court has already found above that the Mandiant Report—incorporated by reference into the Complaint—describe in expert detail the “critical severity” vulnerabilities that were exploited by the data breaches. *See supra* Section III(A)(2).

Accellion also argues that it cannot be liable for an “unfair” act under the WCPA that caused injuries sustained by “downstream” parties, such as Plaintiffs. Reply 12. However, they cite no Washington authority for this proposition, instead only noting that all of Plaintiffs’ WCPA authorities involved data breaches where the defendant had directly collected and stored plaintiffs’ compromised data. *Id.* at 12 n.15. However, Accellion’s role in the data breaches here is analogous to the role of Amazon in the data breach of Capital One’s Amazon Web Services cloud environment where Capital One stored consumers’ confidential PII. *See In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 388 (E.D. Va. 2020). In that case, even though the consumer plaintiffs were also “downstream” parties with respect to Amazon Web Services, the court nonetheless found that the plaintiffs’ WCPA claim to be adequately pled with respect to both Capital One *and Amazon*. *Id.* at 428–29.

Furthermore, as a more general matter, federal courts applying Washington law have consistently found that a “failure to employ adequate data security measures” that “result[s] in harm to thousands of customers” is sufficient to constitute an “unfair” act under the WCPA. *See, e.g., Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1162 (W.D. Wash. 2017) (finding an “unfair act” under WCPA where “the key wrongdoing at issue in this litigation [was] Eddie Bauer’s alleged failure to employ adequate data security measures”) (internal brackets and quotation marks omitted); *Krefting v. Kaye-Smith Enterprises Inc.*, 2023 WL 4846850, at *8 (W.D. Wash. July 28, 2023) (“Under similar circumstances, the Court has found that the failure to take proper measures to secure PII can constitute an unfair act under the [WCPA].”) (collecting cases); *Guy v. Convergent Outsourcing, Inc.*, 2023 WL 4637318, at *8 (W.D. Wash. July 20, 2023) (“Plaintiffs’ allegations of [defendant’s] failure to secure their PII sufficiently identifies an unfair act that satisfies this element of the [WCPA].”); *Buckley v. Santander Consumer USA, Inc.*, 2018 WL 1532671, at *4 (W.D. Wash. Mar. 29, 2018) (“[Defendant’s] alleged ‘failure to take reasonably adequate security measures constitutes an unfair act because it knowingly and foreseeably put [plaintiff] at a risk of harm from data theft and fraudulent . . . activity and this harm allegedly occurred.”).

Given how courts have interpreted and applied Washington law with respect to the WCPA, the Court finds that the Complaint sufficiently alleges an “unfair” act by Accellion in “failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Washington Subclass members’ PII.” Compl. ¶ 235. And because this was the only basis for Accellion’s motion to dismiss the WCPA claim, Accellion’s motion is DENIED with respect to Plaintiffs’ Eleventh Claim for violation of the WCPA.

IV. CONCLUSION

Based on the foregoing, the Court GRANTS IN PART and DENIES IN PART Defendant Accellion’s motion to dismiss, as follows:

1. Accellion’s motion is DENIED as to Plaintiffs’ First Claim for negligence and Eleventh Claim for violations of the WCPA;
2. The Second Claim for negligence per se, the Seventh Claim for breach of contract, and the Twelfth Claim for violations of the MCPA are DISMISSED WITHOUT LEAVE TO AMEND;
3. The Third Claim for violations of the CCPA, the Fourth Claim for violations of the CMIA, the Fifth Claim for violations of the CCRA, the Sixth Claim for intrusion upon seclusion, the Ninth Claim for unjust enrichment, and the Tenth Claim for violations of the California Constitution are DISMISSED WITH LEAVE TO AMEND.

IT IS SO ORDERED.

Dated: January 29, 2024



EDWARD J. DAVILA
United States District Judge