

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DESIREE SCHMITT, et al.,
Plaintiffs,
v.
SN SERVICING CORPORATION, AN
ALASKA CORPORATION,
Defendant.

Case No. [21-cv-03355-WHO](#)

**ORDER DENYING IN PART AND
GRANTING IN PART MOTION TO
DISMISS WITH LEAVE TO AMEND**

Re: Dkt. No. 14

United States District Court
Northern District of California

Plaintiffs Desiree Schmitt and James Furth bring this lawsuit against defendant SN Servicing Corporation (“SNSC”) on behalf of a nationwide class of impacted borrowers for claims arising out of a data breach incident that occurred on SNSC’s system in late 2020. On SNSC’s motion to dismiss, I find that although plaintiffs can assert California law claims as Ohio residents given allegations that SNSC’s principal place of business is in California and that they were harmed by critical decisions SNSC made in California, they fail to plausibly plead the elements of those claims. The negligence claim fails because they do not allege that SNSC had a legal duty to protect the kind of information that was revealed in the data breach. For the same underlying reason, the invasion of privacy claim fails because they do not to allege a serious invasion of a protected privacy interest. And the conclusory allegations they provide are insufficient to state a claim for violation of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200 *et seq.* For the “unlawful” prong, they simply allege that SNSC violated five statutes, without pleading with particularity how the facts of this case pertain to each specific statute and whether the statute can form a basis for a UCL claim. For the “unfair” prong, they do not sufficiently plead policy considerations based on California privacy statutes to satisfy either the “tethering test” or the “balancing test”. Accordingly, SNSC’s motion to dismiss is DENIED in

1 part and GRANTED in part with leave to amend.

2 BACKGROUND

3 SNSC is a financial services corporation that specializes in servicing of residential, small
4 balance commercial, consumer, and unsecured loans. Complaint (“Compl.”) [Dkt. No. 1-1] ¶ 16.
5 It is incorporated in Alaska, with a principal place of business in Eureka, California. *Id.* ¶ 3.
6 Plaintiffs Desiree Schmitt and James Furth are residents of Ohio and were customers of SNSC’s
7 services. *Id.* ¶¶ 1–2.

8 On or about October 14, 2020, a ransomware-threat group known as “Mount Locker” (the
9 “Unauthorized Party”) deployed ransomware into SNSC’s system and successfully acquired a
10 number of digital files maintained by SNSC (hereinafter the “data breach” incident). *Id.* ¶ 62.
11 According to a third-party cybersecurity forensics investigator hired by SNSC, the exfiltration of
12 data from SNSC by the Unauthorized Party ended on or about October 15, 2020. *Id.* ¶ 17.
13 Plaintiffs allege that the Unauthorized Party was able to exfiltrate the “personal and financial
14 information” of approximately 20,155 borrowers, including citizens of the State of California. *Id.*
15 ¶¶ 18–19. Despite learning of the data breach on or around October 15, 2020, SNSC did not send
16 a “Data Beach Notification” letter to plaintiffs and class members until January 14, 2021. *Id.* ¶ 20;
17 *see id.*, Ex. 1.¹

18 The Data Breach Notification letter, which Schmitt and Furth claim they received, states
19 that “the preliminary investigation revealed that the data acquired by the Unauthorized Party
20 includes March 2018 billings statements and fee notices that contain the borrower’s personal and
21 financial information including, among other information, borrower names, addresses, loan
22 numbers, balance information, and billing information such as charges assessed, owed, and/or
23 paid.” *Id.* ¶¶ 22, 40, 45. The Data Breach Notification letter further states that “SNSC is still in
24 the process of conducting an investigation of the incident to determine if additional personal and
25 financial information pertaining to [plaintiffs] was exfiltrated.” *Id.* ¶¶ 40, 45. In a separate

26
27 ¹ This case was removed from San Francisco County Superior Court. The Data Breach
28 Notification letter is not attached to the Complaint submitted along with SNSC’s Notice of
Removal. Plaintiffs shall attach a copy of the Data Breach Notification letter to their amended
pleading so that it is properly before this court.

1 January 14, 2021 letter to the New Hampshire Attorney General, SNSC stated that “it had hired a
2 third party e-discovery vendor to conduct a ‘data mining’ review of the documents that were
3 identified to have been exfiltrated to determine whether additional personal and financial
4 information was compromised.” *Id.*

5 Plaintiffs allege that personal and financial information is “such a valuable commodity to
6 identity thieves that once information has been compromised, criminals often trade the
7 information on the ‘cyber black-market’ for years.” *Id.* ¶ 34. Accordingly, they contend, there is
8 a “strong probability” that their stolen information is, or soon will be, on the cyber black-market,
9 placing them and other class members “at an increased risk of fraud and identity theft for many
10 years into the future.” *Id.* ¶ 35. As a result of the data breach, and as recommended by the Data
11 Breach Notification letter, plaintiffs assert that they must now be “vigilant and review their credit
12 reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts,
13 and other steps to protect themselves against identity theft.” *Id.* ¶ 24.

14 In particular, Schmitt alleges that she “purchased credit monitoring with Lifelock at an
15 annual cost of more than \$200.00, as well as LastPass password manager, which is a monthly
16 password manager and password vault application subscription service that costs \$3.00 per month,
17 and YubiKey password protection at a cost of more than \$90.00.” *Id.* ¶ 41. Furth contends that he
18 too “purchased Lifelock identify protection at an annual cost of \$99.48” after the data breach. *Id.*
19 ¶ 46. Both claim that they have “spent time and energy protecting and monitoring [their] identity
20 and credit” and will have to “spend additional time and energy in the future continuing to monitor
21 and protect [their] identity and credit.” *Id.* ¶¶ 42, 47. Schmitt alleges that she “spent at least 10
22 hours changing hundreds of passwords related to her business and personal accounts.” *Id.* ¶ 42.
23 Both allege that they “suffered anxiety, emotional distress, and loss of privacy” as a result of the
24 data breach. *Id.* ¶¶ 42, 47.

25 Plaintiffs claim that SNSC started to undertake the “basic steps” recognized in the industry
26 to protect their and other class members’ personal and financial information only after an
27 Unauthorized Party was able to exfiltrate a large amount of data. *Id.* ¶ 23. As the Data Breach
28 Notification letter indicates, SNSC began bolstering its cybersecurity posture after the data breach

1 incident “by replacing email filtering tools, malware software, and Internet monitoring tools with
2 more robust solutions that utilizes AI to detect and block known and newly introduced malware,
3 and block all inbound and outbound Internet, email, and network traffic to foreign countries.” *Id.*
4 Because of SNSC’s failure to “create, maintain, and/or comply with necessary cybersecurity
5 requirements,” plaintiffs allege that SNSC “was unable to protect borrower’s information and
6 confidentiality, and protect against obvious and readily foreseeable threats to information security
7 and confidentiality or unauthorized access to personal and financial information, resulting in the
8 Data Breach.” *Id.* ¶ 27.

9 Plaintiffs filed this lawsuit in San Francisco County Superior Court on March 12, 2021,
10 bringing the following three claims on behalf a nationwide class of borrowers impacted by the
11 data breach: (i) negligence; (ii) invasion of privacy; and (iii) relief under the “unlawful” and
12 “unfair” prongs of the UCL. On May 5, 2021, SNSC removed the action to this court and
13 subsequently filed a motion to dismiss for failure to state a claim. Notice of Removal [Dkt. No.
14 1]; Defendant SN Servicing Corporation’s Motion to Dismiss Plaintiffs’ Complaint [Dkt. No. 14].

15 LEGAL STANDARD

16 Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint
17 if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to
18 dismiss, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its
19 face.” *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible
20 when the plaintiff pleads facts that “allow the court to draw the reasonable inference that the
21 defendant is liable for the misconduct alleged.” *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)
22 (citation omitted). There must be “more than a sheer possibility that a defendant has acted
23 unlawfully.” *Id.* While courts do not require “heightened fact pleading of specifics,” a plaintiff
24 must allege facts sufficient to “raise a right to relief above the speculative level.” *See Twombly*,
25 550 U.S. at 555, 570.

26 In deciding whether the plaintiff has stated a claim upon which relief can be granted, the
27 court accepts the plaintiff’s allegations as true and draws all reasonable inferences in favor of the
28 plaintiff. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court

1 is not required to accept as true “allegations that are merely conclusory, unwarranted deductions of
 2 fact, or unreasonable inferences.” *See In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir.
 3 2008).

4 DISCUSSION

5 I. CALIFORNIA CLAIMS BY NON-CALIFORNIA PLAINTIFFS

6 While California has a presumption against extraterritorial application of its own law,
 7 *Sullivan v. Oracle Corp.*, 51 Cal.4th 1191, 1207 (2011), “state statutory remedies may be invoked
 8 by out-of-state parties when they are harmed by wrongful conduct occurring in California.” *In re*
 9 *iPhone 4S Consumer Litig.*, No. C 12-1127 CW, 2013 WL 3829653, at *7 (N.D. Cal. Jul. 23,
 10 2013) (quoting *Norwest Mortg., Inc. v. Superior Ct.*, 72 Cal. App. 4th 214, 224–225 (1999)). To
 11 determine whether sufficient wrongful conduct occurred in California, “courts consider where the
 12 defendant does business, whether the defendant’s principal offices are located in California, where
 13 class members are located, and the location from which . . . decisions were made.” *In re Toyota*
 14 *Motor Corp.*, 785 F. Supp. 2d 883, 917 (C.D. Cal. 2011).

15 Plaintiffs offer the following to establish the nexus between California and the alleged
 16 wrongful conduct: (i) SNSC’s principal place of business is in Eureka, California; (ii) the “nerve
 17 center” of SNSC’s activities is in California, “the place where its high-level officers direct,
 18 control, and coordinate the company’s activities, including its data security functions and policy,
 19 financial, and legal decisions”; and (iii) SNSC’s response to the Data Breach at issue here,
 20 including investigation and notification to plaintiffs and class members from California, were
 21 made from and in California. *See* Compl. ¶¶ 56–61.

22 Other courts have found similar allegations sufficient to allow out-of-state plaintiffs to
 23 seek recovery under California law. *See, e.g., Ehret v. Uber Techs., Inc.*, 68 F. Supp. 3d 1121,
 24 1132 (N.D. Cal. 2014) (finding “sufficient nexus between California and the misrepresentations
 25 which form the basis of Plaintiff’s claims,” where plaintiffs alleged that the deceptive practices
 26 were controlled from Uber’s headquarters in San Francisco, California and the transactions for
 27 Uber’s services were processed in its servers there); *In re iPhone 4S Consumer Litig.*, 2013 WL
 28 3829653, at *7 (out-of-state plaintiffs had standing to prosecute UCL and other California

1 statutory claims because their alleged injuries were caused by Apple’s wrongful conduct in false
2 advertising that originated in California); *In re Mattel*, 588 F. Supp. 2d 1111, 1119 (C.D. Cal.
3 2008) (out-of-state plaintiffs could bring California state law claims because they complained of
4 “misrepresentations made in reports, company statements, and advertising that are reasonably
5 likely to have come from or been approved by Mattel corporate headquarters in California”).

6 Plaintiffs also cite other data breach cases that have similarly applied the law of the state
7 where the company had its headquarters. *See, e.g., In re Premera Blue Cross Customer Data Sec.*
8 *Breach Litig.*, No. 3:15-MD-2633-SI, 2019 WL 3410382, at *14 (D. Or. Jul. 29, 2019) (although
9 some conduct underlying plaintiffs’ negligence claim occurred by others in other locations,
10 including plaintiffs providing their information in their home states and the hackers engaging in
11 conduct in China, the alleged negligent conduct originated in the defendant company’s
12 headquarters in Washington, including decisions that led to the data breach); *First Choice Fed.*
13 *Credit Union v. Wendy’s Co.*, No. CV 16-506, 2018 WL 2729264, at *6–7 (W.D. Pa. May 9,
14 2018), *report and recommendation adopted*, No. CV 16-506, 2018 WL 2721998 (W.D. Pa. Jun. 6,
15 2018) (finding the most significant factor in choice-of-law analysis in a data breach class action is
16 the place of the alleged conduct that caused injury, *i.e.*, “the alleged actions and inactions of
17 Defendants at issue in this case took place at Defendants’ headquarters in Ohio”); *In re Target*
18 *Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 486 (D. Minn. Sept. 15, 2015) (place of
19 corporation’s headquarters, where the computer servers were located and where decision regarding
20 the data breach were made, constituted sufficient contacts to apply state law to out-of-state
21 plaintiffs’ claims).

22 SNSC does not dispute the case law cited above. In its reply brief, it only focuses on
23 plaintiffs’ additional allegation that the choice-of-law provision in SNSC’s Terms and Conditions
24 selects California law. *See* Compl. ¶ 61. While a selected choice-of-law provision may be
25 insufficient on its own to create a nexus to California and confer standing on out-of-state residents,
26 plaintiffs here have alleged more. *See In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *7.

27 SNSC’s motion to dismiss on this ground is DENIED. As noted below, however, plaintiffs
28 run into a potential pleading problem by relying on certain California data breach laws to the

1 extent that those laws only cover California residents.

2 **II. NEGLIGENCE**

3 **A. Duty of Care**

4 SNSC argues that the California legislature limited duty “to provide reasonable security”
 5 to only certain types of sensitive personal identifying information (“PII”), not all personal data.
 6 *See* Cal. Civ. Code § 1798.81.5(d)(1). An actionable data breach must result in the disclosure of a
 7 person’s name together with one of the following identifiers: (i) social security number, (ii)
 8 government-issued ID number, (iii) financial account number in combination with a code “or
 9 password that would permit access to an individual’s financial account,” (iv) biometric data, (v)
 10 medical and health insurance information, or (vi) an email or user name with a password
 11 combination that would permit account access. *See id.* Because plaintiffs only allege the
 12 disclosure of “borrower names, addresses, loan numbers, balance information, and billing
 13 information such as charges assessed, owed, and/or paid,” none of which amounts to a disclosure
 14 of PII, SNSC contends that a legal duty has been inadequately pleaded. Compl. ¶¶ 22, 40, 45.

15 Plaintiffs analogize their case to *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1031 (N.D.
 16 Cal. 2019), where the information consisted of, among other things, names, phone numbers or
 17 email addresses, gender, dates of birth, the types of devices used to access Facebook, and the last
 18 ten places the user “checked into” or was “tagged” in on Facebook. They summarily argue that
 19 the compromised information here is similarly “immutable,” and therefore highly valuable,
 20 without explaining how access to names, addresses, loan numbers, balance information, and
 21 billing information can be considered “ammo” to commit future fraud as it did in *Bass*. *Id.* at
 22 1035.

23 The plaintiff in *Bass* supported his negligence claim by engaging with the “*Rowland*
 24 factors” that California courts consider when determining the existence of a legal duty. *See*
 25 *Regents of Univ. of Cal. v. Superior Court*, 4 Cal. 5th 607, 628 (2018) (factors include “the
 26 foreseeability of harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the
 27 closeness of the connection between the defendant’s conduct and the injury suffered, the moral
 28 blame attached to the defendant’s conduct, the policy of preventing future harm, the extent of the

1 burden to the defendant and the consequences to the community of imposing a duty to exercise
2 care with resulting liability for breach, and the availability, cost, and prevalence of insurance for
3 the risk involved) (citing *Rowland v. Christian*, 69 Cal.2d 108, 113 (1968)). The *Bass* court found
4 that “[t]hese factors have been satisfied” because “[t]he lack of reasonable care in the handling of
5 personal information can foreseeably harm the individuals providing the information” and
6 “[f]urther, some of the information [at issue] was private, and plaintiff plausibly placed trust in
7 Facebook to employ appropriate data security.” *Bass*, 394 F. Supp. 3d at 1039. Plaintiffs here fail
8 to engage in a similar analysis using the *Rowland* factors.

9 For the first time in their opposition, plaintiffs assert that their social security numbers
10 were also compromised. That allegation appears nowhere in the Complaint. Plaintiffs do allege,
11 however, that there is likely more data stolen than they know about because, as of January 14,
12 2021, SNSC indicated that it is still determining “whether additional personal and financial
13 information was compromised.” Compl. ¶ 22. Without the benefit of discovery or further
14 investigation, plaintiffs argue that they are unable to specifically allege whether additional
15 personal and financial information, like social security numbers, was compromised.

16 I understand that plaintiffs are working with limited information at this juncture. That
17 said, they need to provide more factual allegations from which I can draw a reasonable inference
18 that PII (information SNSC had a legal duty to protect) was among the information compromised
19 during the data breach. They can do so by, for example, pleading what kind of information they,
20 and customers like them, provided to SNSC. With allegations that certain less sensitive
21 information was released during the data breach (per the Data Breach Notification letter) and that
22 SNSC at least had in its possession other more sensitive information (which rise to the level of
23 PII), a reasonable inference could be drawn that PII was also among the information compromised
24 during the data breach.

25 **B. Breach**

26 Assuming that plaintiffs can allege a plausible legal duty on amendment, I note that their
27 burden to plead a corresponding breach based on SNSC’s inadequate security measures is not
28 high. Another data breach case out of this District recognized as much:

1 The consuming public has come to believe that the internet
2 companies, which take in their private information, have taken
3 adequate security steps to protect the security of that information from
4 any and all hackers or interventions. The ordinary consumer,
5 however, has no clue what internet companies' security steps are.
6 There would be no way for users to know what security steps were
7 actually in place. Therefore, when a breach occurs, *the thing speaks*
8 *for itself*. The breach would not have occurred but for inadequate
9 security measures, or so it can be reasonably inferred at the pleadings
10 stage.

11 *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30,
12 2021).

13 SNSC distinguishes *Flores-Mendez* on grounds that the data breach in that case involved
14 highly "sensitive information about sexual preferences, which . . . could plausibly lead to
15 blackmail and embarrassment." *Id.* The distinction in the type of information released only shows
16 why plaintiffs have not plausibly pleaded the duty element of their claim, as discussed above. It
17 does not undermine the point that plaintiffs need not cross a high bar to plead a corresponding
18 breach once they are able to allege a valid legal duty to maintain their negligence claim.

19 **C. Causation and Damages**

20 I address the remaining negligence elements with the same assumption that plaintiffs are
21 able to allege a valid legal duty and that the information revealed during the data breach
22 sufficiently constitutes PII.

23 "Under California law, appreciable, nonspeculative, present harm is an essential element of
24 a negligence cause of action." *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 649 (N.D. Cal. 2020)
25 (citing *Aas v. Super. Ct.*, 24 Cal. 4th 627, 646 (2000), *superseded by statute on other grounds*, Cal.
26 Civ. Code § 895 *et seq.*, *as recognized in S. Cal. Gas Leak Cases*, 7 Cal. 5th 391, 412 (2019)).
27 Plaintiffs allege they have suffered actual damages in the following forms: "imminent risk of
28 identify theft; expenses and/or time spent on credit monitoring for a period of years; time spent
scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud
alerts and credit freezes and subsequently temporarily lifting credit freezes; an increased risk of
future harm," "anxiety, emotional distress, loss of privacy, and other economic and non-economic
losses." Compl. ¶ 79. SNSC argues that voluntarily purchasing credit monitoring cannot suffice

1 as cognizable damages, particularly when plaintiffs have not alleged that their PII was actually
2 stolen as a result of the data breach.

3 A similar argument was raised in *Huynh*, 508 F. Supp. 3d at 649, where the defendant
4 moved for summary judgment on a data breach negligence claim because “Plaintiff has not
5 suffered identity theft and asserts that she has voluntarily attempted to repair any hypothetical
6 threat of future harm by temporarily purchasing credit monitoring services and monitoring her
7 accounts.” The court noted that “California courts have not considered whether time and money
8 lost to credit monitoring from the future threat posed by compromised PII are damages to support
9 a negligence claim,” but, after considering the case law, concluded that “time and money [the
10 plaintiff] spent on credit monitoring in response to the Data Breach is cognizable harm to support
11 her negligence claim.” *Id.* at 649–50. “Increased time spent monitoring one’s credit and other
12 tasks associated with responding to a data breach have been found by other[] courts to be specific,
13 concrete, and non-speculative.” *In re Solara Med. Supplies, LLC Customer Data Sec. Breach*
14 *Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020) (citing cases,
15 including *Bass*, 394 F. Supp 3d at 1039); *see also Castillo v. Seagate Tech., LLC*, No. 16-CV-
16 01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (finding cognizable injury where
17 some plaintiffs bought a subscription to an identity protection service “because they wanted
18 greater protection than that offered” by the defendant). The money and time plaintiffs spent on
19 credit monitoring are both cognizable forms of harm.

20 SNSC further argues that the negligence claim is barred by the economic loss doctrine
21 because plaintiffs do not allege strictly economic losses. It primarily relies on one case from the
22 Southern District in support of this argument. *See Dugas v. Starwood Hotels & Resorts*
23 *Worldwide, Inc.*, No. 316CV00014GPCBLM, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016)
24 (finding plaintiffs alleged “nothing more than pure economic loss” and “no personal injury or
25 physical damage to property” where plaintiffs alleged injuries in the form of “theft of their credit
26 card information, costs associated with prevention of identity theft, and costs associated with time
27 spent and loss of productivity, among other injuries”).

28 Recent cases out of this District, however, have found that the economic loss doctrine does

1 not apply where loss of time is alleged, as plaintiffs have alleged here. *See, e.g., Bass*, 394 F.
2 Supp. 3d at 1039 (“Here, plaintiff alleged his loss of time as a harm and so does not allege pure
3 economic loss. The economic loss rule therefore does not apply.”); *Huynh*, 508 F. Supp. 3d at 654
4 (“This Court previously held that the economic loss rule did not bar Plaintiff’s negligence claim
5 because she alleged loss of time as a harm, meaning she had not alleged pure economic loss.”); *see*
6 *also Flores-Mendez*, 2021 WL 308543, at *4 (“[P]laintiffs adequately allege damages in the form
7 of a heightened risk of future identity theft, loss of privacy with respect to highly sensitive
8 information, loss of time, and risk of embarrassment.”). Other judges in the Southern District
9 have also found the same in more recent opinions. *See, e.g., In re Solara Med. Supplies, LLC*
10 *Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *4 (S.D.
11 Cal. May 7, 2020) (finding the economic loss doctrine does not apply because “[p]laintiffs have
12 alleged they have lost time responding to the Breach as well as suffering from increased anxiety
13 and so do not allege purely economic losses”).

14 With respect to the causation element, SNSC argues that plaintiffs have not made the
15 requisite connection between the alleged breach and damages because they do not assert that they
16 were victims of identity theft or fraud following the data breach or ruled out alternative causes by
17 pleading that they did not suffer identity theft or fraud prior to the data breach. Without
18 allegations of an actual improper use of their PII and lack of prior identify theft incidents, SNSC
19 argues that the negligence claim must fail.

20 To the extent SNSC’s causation argument relies on the premise that plaintiffs must allege
21 an actual identity theft or fraud to maintain their negligence claim, it is flawed for the same
22 reasons discussed above regarding cognizable injuries. To the extent the argument is premised on
23 whether plaintiffs’ decision to purchase credit monitoring services and spend time mitigating risk
24 of harm was “reasonable” or “necessary” given the type of information revealed in the data
25 breach, I agree that plaintiffs’ allegations are lacking. Because plaintiffs have not plausibly
26 pleaded that PII or identifiable information was disclosed (information that SNSC had a duty to
27 protect), they have not plausibly pleaded that their decision to purchase credit monitoring services
28 and spend time mitigating any risk of harm after the data breach was reasonable or necessary. But

1 if they plausibly plead that their PII was compromised, a reasonable inference would follow that
2 their decision to purchase monitoring services was “reasonable” and “necessary.”

3 SNSC’s motion to dismiss the negligence claim is GRANTED with leave to amend.

4 **III. INVASION OF PRIVACY**

5 Under California law, to adequately state a claim for invasion of privacy, a plaintiff must
6 demonstrate three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of
7 privacy under the circumstances; and (3) a serious invasion of the privacy interest. *In re iPhone*
8 *Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing *Hill v. Nat’l Collegiate*
9 *Athletic Assn.*, 7 Cal. 4th 1, 35–37 (1994)). SNSC challenges the third element of plaintiff’s
10 claim.

11 Actionable invasions of privacy must be sufficiently “serious in their nature, scope, and
12 actual or potential impact to constitute an *egregious* breach of the social norms underlying the
13 privacy right.” *Hill*, 7 Cal.4th at 26 (finding rules requiring college football players to submit to
14 drug testing were not egregious breaches of social norms) (emphasis added); *Low v. LinkedIn*
15 *Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (recognizing a “high bar” for pleading
16 invasion of privacy claims) (citing cases). “Even negligent conduct that leads to theft of highly
17 personal information, including social security numbers, does not ‘approach [the] standard’ of
18 actionable conduct under the California Constitution and thus does not constitute a violation of
19 Plaintiffs’ right to privacy.” *iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (quoting *Ruiz v.*
20 *Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008) *aff’d*, 380 Fed. Appx. 689 (9th Cir.
21 2010)).

22 Plaintiffs contend that the criminal nature of the data breach and the information that was
23 exposed or stolen in the data breach demonstrates that SNSC committed a serious violation of
24 their privacy rights. Courts faced with similar data breach scenarios have found such allegations
25 insufficient. *See, e.g., Razuki v. Caliber Home Loans, Inc.*, No. 17CV1718-LAB (WVG), 2018
26 WL 2761818, at *2 (S.D. Cal. Jun. 8, 2018) (“Losing personal data through insufficient security
27 doesn’t rise to the level of an egregious breach of social norms underlying the protection of
28 sensitive data like social security numbers [plaintiff’s] allegations don’t suggest the type of

1 intentional, egregious privacy invasion contemplated in *Hill.*”); *In re iPhone Application Litig.*,
2 844 F. Supp. 2d at 1063 (finding information disclosed to third parties, including unique device
3 identifier number, personal data, and geolocation information, did not constitute an egregious
4 breach of social norms).

5 The cases plaintiffs cite are easily distinguishable. The invasion of privacy claim in *Doe v.*
6 *Beard*, 63 F. Supp. 3d 1159, 1170 (C.D. Cal. 2014) involved the disclosure of medical
7 information, including the plaintiff’s HIV-positive status, and thus was subject to a “lower
8 threshold” for “egregious violations of social norms.” Similarly, *Stasi v. Inmediata Health Grp.*
9 *Corp.*, 501 F. Supp. 3d 898, 926 (S.D. Cal. 2020) recognized that “some courts have dismissed
10 privacy claims based on the state constitution given the ‘high bar’ for such claims,” but
11 distinguished those cases on grounds that they “[did] not involve[] medical information that was
12 ‘posted’ on the internet.” Plaintiffs’ remaining citations are outside the data breach context and,
13 unlike the (at most) negligent conduct alleged here, those cases involved intentional disclosures of
14 privileged information. See *Strawn v. Morris, Polich & Purdy, LLP*, 30 Cal. App. 5th 1087,
15 1093–98 (2019) (plaintiffs alleged that a State Farm representative demanded privileged tax
16 returns from defendants and intentionally disclosed them to third parties); *In re Facebook, Inc.*
17 *Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020) (plaintiffs challenged Facebook’s use of
18 programs to track users’ web browsing and intentional accumulation of consumer information for
19 sale to third parties).

20 Because plaintiffs have failed to establish that SNSC’s conduct amounts to a serious
21 invasion of a protected privacy interest, SNSC’s motion to dismiss the invasion of privacy claim is
22 GRANTED with leave to amend.

23 **IV. UCL**

24 **A. Standing**

25 To establish standing under the UCL, a plaintiff’s claim must specifically involve lost
26 money or property. See *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011); *Ehret v. Uber*
27 *Techs., Inc.*, 68 F. Supp. 3d 1121, 1132 (N.D. Cal. 2014) (“Whereas a federal plaintiff’s injury in
28 fact may be intangible and need not involve lost money or property, . . . a UCL plaintiff’s injury in

1 fact [must] specifically involve lost money or property.”) (internal quotation marks omitted).

2 In the data breach context, “payments toward enhanced credit monitoring that arise from a
3 data breach and that are not reimbursed [] constitute economic injury, sufficient to confer UCL
4 standing.” *Huynh*, 508 F. Supp. 3d at 661 (internal quotation marks and citation omitted). That is
5 exactly what plaintiffs have alleged here—both plaintiffs bought enhanced credit monitoring
6 protection and other services after the data breach incident. *See* Compl. ¶¶ 41, 46; *In re Marriott*
7 *Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 492 (D. Md. 2020) (lost money
8 or property is sufficiently alleged where a plaintiff is “required to enter into a transaction, costing
9 money or property, that would otherwise have been unnecessary”) (quoting *Kwikset*, 51 Cal. 4th at
10 323).

11 SNSC distinguishes the summary judgment ruling in *Huynh* on grounds that plaintiffs here
12 did not seek reimbursements from SNSC for the credit monitoring services they purchased.
13 *Huynh* did not turn on whether plaintiffs directly sought reimbursements from the defendant
14 company. Indeed, the line of cases cited in *Huynh* suggest that plaintiffs’ allegations are sufficient
15 for pleading purposes.² To the extent that SNSC factually disputes whether plaintiffs’ credit
16 monitoring costs were “required” or “necessary,” that cannot be resolved that this stage.

17 The two cases SNSC provides are distinguishable. In *Dugas v. Starwood Hotels & Resorts*
18 *Worldwide, Inc.*, 2016 WL 6523428, at *11, the plaintiff only generally alleged that “unauthorized
19

20 _____
21 ² *See In re Yahoo! Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL
22 3727318, *21–22 (N.D. Cal. Aug. 30, 2017) (finding plaintiffs incurred out-of-pocket expenses on
23 credit monitoring services after the data breach incident and therefore were “required to enter into
24 a transaction, costing money or property, that would otherwise have been unnecessary”); *In re*
25 *Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 986–87 (N.D. Cal. 2016) (finding the
26 language in *Kwikset* favors the argument that money spent on credit monitoring to prevent fraud is
27 sufficient to assert statutory standing under the UCL); *Corona v. Sony Pictures Ent., Inc.*, No. 14-
28 CV-09600 RGK EX, 2015 WL 3916744, at *5, *8 (C.D. Cal. Jun. 15, 2015) (finding UCL
standing sufficiently alleged based on “costs relating to credit monitoring, identity theft protection,
and penalties”); *Witriol v. LexisNexis Grp.*, No. C05-02392 MJJ, 2006 WL 4725713, *6 (N.D.
Cal. Feb. 10, 2006) (finding “costs associated with monitoring and repairing credit impaired by the
unauthorized release of private information” constitute “monetary loss as a result of Defendants’
actions”); *Walters v. Kimpton Hotel & Rest. Grp., LLC*, No. 16-CV-05387-VC, 2017 WL
1398660, at *2 (N.D. Cal. Apr. 13, 2017) (finding plaintiff sufficiently alleged economic injury
resulting from breach to maintain UCL claim, including having to secure and maintain credit
monitoring services and other out-of-pocket expenses and the value of time reasonably incurred to
remedy or mitigate the breach) (internal quotation marks citation omitted).

1 charges were made on his credit card, that he will incur damages to monitor identity theft, and that
 2 he has spent time responding to the unauthorized charges on his credit card.” In *Bass*, 394 F.
 3 Supp. 3d at 1040, the plaintiff implausibly alleged “(i) loss of the value of the personal
 4 information and (ii) failure to receive the benefit of his bargain with Facebook,” and did not claim
 5 any costs associated with credit monitoring.

6 SNSC’s motion to dismiss the UCL claim for lack of statutory standing is DENIED.

7 **B. Unlawful Prong**

8 The unlawful prong of the UCL prohibits “anything that can properly be called a business
 9 practice and that at the same time is forbidden by law.” *In re Yahoo! Inc. Customer Data Sec.*
 10 *Breach Litig.*, 2017 WL 3727318, at *23 (citation omitted). By proscribing “any unlawful”
 11 business practice, the UCL permits injured consumers to “borrow” violations of other laws and
 12 treat them as unlawful competition that is independently actionable. *Id.*

13 As predicates for their UCL claim under the unlawful prong, plaintiffs allege that SNSC
 14 violated five statutes in failing to implement reasonable security measures and safeguard
 15 customers’ data: (i) section 5 of the Federal Trade Commission (“FTC”) Act, 15 U.S.C. § 45; (ii)
 16 and (iii) provisions of the California Customer Records Act (“CRA”), Cal. Civ. Code §§
 17 1798.81.5, 1798.82; (iv) the California Financial Information Privacy Act (“FIPA”), Cal. Fin.
 18 Code § 4052.5, and (v) an Ohio statute, Ohio Rev. Code 1349.19, that requires disclosure of
 19 breach of security system. *See* Compl. ¶¶ 86–89.

20 A UCL claim of any kind “must identify the particular section of the statute that was
 21 violated and must describe with reasonable particularity the facts supporting the violation.” *Bros.*
 22 *v. Hewlett-Packard Co.*, No. C-06-02254 RMW, 2006 WL 3093685, at *7 (N.D. Cal. Oct. 31,
 23 2006) (applying *Khoury v. Maly’s of California, Inc.*, 14 Cal. App. 4th 612, 619 (1993)).
 24 Plaintiffs fail to do that here. They broadly claim that SNSC violated all five statutes by, among
 25 other things, “[f]ailing to establish adequate practices and procedures for maintaining and storing
 26 Plaintiffs’ and Class members’ personal and financial information, and storing Plaintiffs’ and
 27 Class members’ personal and financial information in an unsecure electronic environment.” *See*
 28 Compl. ¶ 86(a). Such conclusory allegations do not suffice. *See Baba v. Hewlett-Packard Co.*,

1 No. C 09-05946 RS, 2010 WL 2486353, at *6 (N.D. Cal. Jun. 16, 2010) (dismissing UCL claim
 2 where plaintiffs conclusorily alleged that defendants violated six statutes without considering that
 3 each “has its own line of case law and its own set of elements” and requiring plaintiffs to “plead
 4 with particularity how the facts of this case pertain to that specific statute”).

5 In addition to the conclusory nature of plaintiffs’ allegations, SNSC further argues that
 6 plaintiffs cannot state a claim under any of the five statutes because many of them do not confer a
 7 private right of action. Plaintiffs respond that a private right of action is not required for a statute
 8 to form a basis for an unlawful UCL violation. For example, the data breach plaintiffs in
 9 *Anthem*, 162 F. Supp. 3d at 989, pleaded unlawful conduct as violations of the FTC Act and other
 10 statutes, even though those statutes did not provide a private right of action. Thus, plaintiffs
 11 argue, “[i]t does not follow” that a private UCL action cannot borrow from another law
 12 enforceable only by public lawyers. *LegalForce RAPC Worldwide P.C. v. UpCounsel, Inc.*, No.
 13 18-cv-02573-YGR, 2019 WL 160335, at * 14 (N.D. Cal. Jan. 10, 2019) (quoting *Stop Youth*
 14 *Addiction, Inc. v. Lucky Stores, Inc.*, 17 Cal. 4th 553, 566 (1998)).

15 SNSC contends that plaintiffs’ citations contradict the well-established principle that
 16 plaintiffs cannot use the UCL “to engineer” a private right of action when the underlying statute
 17 does not create it. *O’Donnell v. Bank of Am., Nat. Ass’n*, 504 Fed. Appx. 566, 568 (9th Cir. 2013).
 18 The Ninth Circuit in *O’Donnell* upheld the district court’s dismissal of a UCL claim premised on
 19 the defendants’ alleged violation of the FTC Act, reasoning that the “federal statute doesn’t create
 20 a private right of action” and “plaintiffs can’t use California law to engineer one.” *Id.* (citing
 21 *Carlson v. Coca-Cola Co.*, 483 F.2d 279, 280 (9th Cir.1973), and *Lucia v. Wells Fargo Bank,*
 22 *N.A.*, 798 F.Supp.2d 1059, 1072 (N.D. Cal. 2011) *reversed on other grounds*, 728 F.3d 878 (9th
 23 Cir. 2013)).

24 It appears that the district court’s ruling in *Anthem*, 162 F. Supp. 3d at 989, where an
 25 unlawful UCL claim predicated on the FTC Act was not dismissed, conflicts with the Ninth
 26 Circuit’s disposition in *O’Donnell*, where dismissal of unlawful UCL claim predicated on the FTC
 27 Act was upheld. Notably however, the district court in *Anthem* did not directly address whether
 28 the FTC Act created a private right of action or expressly prohibited it. *See LegalForce*, 2019 WL

1 160335, at *13 (“[I]f a statute explicitly precludes private enforcement, or if a statute expressly
 2 provides immunity for the conduct alleged, a plaintiff may not plead around this bar by bringing a
 3 claim under the UCL.”). The *Anthem* court only stated that “a review of the complaint
 4 demonstrates that Plaintiffs’ allegations ‘identify the particular section of the statute that was
 5 violated,’ and other allegations in the consolidated amended complaint ‘describe with reasonable
 6 particularity the facts supporting the violation.’” *Anthem*, 162 F. Supp. 3d at 989 (quoting *Baba*,
 7 2010 WL 2486353, at *6). The Ninth Circuit’s ruling in *O’Donnell*, therefore, carries more
 8 persuasive weight here. For purposes of alleging an unlawful business practice, plaintiffs cannot
 9 predicate their UCL claim on the FTC Act. But, as discussed below, they may be able to use the
 10 FTC Act to allege a claim under the unfair prong.

11 The applicability of the remaining four statutes, which plaintiffs fail to address in their
 12 opposition, is also questionable. SNSC argues that plaintiffs cannot use the CRA, California Civil
 13 Code sections 1798.81.5 and 1798.82, as predicates because they have not alleged how SNSC
 14 violated those statutes. The case law suggests that non-California plaintiffs cannot use the CRA
 15 provisions to predicate their UCL “unlawful” claim. *See In re Yahoo! Inc. Customer Data Sec.*
 16 *Breach Litig.*, 2017 WL 3727318, at *34 (dismissing standalone claims brought under California
 17 Civil Code section 1798.82 because “non-California residents lack standing to bring claims under
 18 the CRA”); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 942,
 19 973 (S.D. Cal. Oct. 11, 2012) (dismissing CRA claims brought on behalf of non-California
 20 plaintiffs because the CRA “is clear that it applies only ‘to ensure the personal information [of]
 21 California residents is protected’”) (quoting Cal. Civ. Code § 1798.81.5(a)); *see also Antman v.*
 22 *Uber Techs., Inc.*, No. 3:15-CV-01175-LB, 2015 WL 6123054, at *5 (N.D. Cal. Oct. 19, 2015)
 23 (“Section 1798.82 has procedures for notifying *California residents* when their unencrypted
 24 personal information is disclosed in a data breach and thereby acquired (or reasonably believed to
 25 have been acquired by) an unauthorized person.”) (citing Cal. Civ. Code § 1798.82(a) (emphasis
 26 added)).

27 Plaintiffs similarly fail to explain how the data breach conduct alleged here is within the
 28 scope of the FIPA, California Financial Code section 4052.5, which “prohibit[s] financial

1 institutions from disclosing nonpublic personal information with ‘nonaffiliated third parties.’”
 2 *Park v. Wells Fargo Bank*, No. C 12-2065 PJH, 2012 WL 3309694, at *4 (N.D. Cal. Aug. 13,
 3 2012) (citing Cal. Fin. Code § 4052.5). Nor do they explain why UCL violations can be
 4 predicated on another state’s law, such as Ohio Rev. Code Ann. 1349.19.

5 SNSC’s motion to dismiss the UCL claim under the unlawful prong is GRANTED with
 6 leave to amend.

7 **C. Unfair Prong**

8 The unfair prong of the UCL creates a cause of action for a business practice that is unfair
 9 even if not proscribed by some other law. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*,
 10 2017 WL 3727318, at *23 (citing *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134,
 11 1143 (2003). “The UCL does not define the term ‘unfair’ . . . [and] the proper definition of
 12 ‘unfair’ conduct against consumers ‘is currently in flux’ among California courts.” *Id.*

13 Some California courts apply a balancing approach, which requires courts to “weigh the
 14 utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Davis v.*
 15 *HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (internal quotation marks
 16 omitted). Other California courts have held that “unfairness must be tethered to some legislatively
 17 declared policy or proof of some actual or threatened impact on competition.” *Lozano v. AT & T*
 18 *Wireless Servs., Inc.*, 504 F.3d 718, 735 (9th Cir. 2007) (internal quotation marks omitted). These
 19 tests are typically referred to as the “balancing test” and the “tethering test”.

20 Under the tethering test, plaintiffs argue that they “need merely to show that the effects of
 21 [SNSC’s] conduct ‘are comparable to or the same as a violation of the law, or otherwise
 22 significantly threaten or harm competition.’” *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197,
 23 1227 (N.D. Cal. 2014) (quoting *Cel-Tech Commc’ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal.
 24 4th 163, 187 (1999)) (internal alterations omitted). They contend that the effects of SNSC’s
 25 conduct are comparable to a violation of the five laws mentioned in the Complaint—including 15
 26 U.S.C. § 45, Cal. Civ. Code 1798.81.5–82, Cal. Fin. Code § 4052.5, and Ohio Rev. Code §
 27 1349.19—which impose duties to maintain reasonable security over consumers’ personal
 28 identifying information and require reasonable notification if a data breach occurs. As discussed

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

above, their allegations with respect to these five statutes are vague and conclusory.

Plaintiffs “may proceed with a UCL claim under the balancing test by either alleging immoral, unethical, oppressive, unscrupulous or substantially injurious conduct by Defendants or by demonstrating that Defendants’ conduct violated an established public policy.” *Anthem*, 162 F. Supp. 3d at 990. For example, the plaintiffs in *In re Yahoo!* sufficiently pleaded an unfair business practice by alleging that “Defendants promised in their Privacy Policy to protect their customers ‘data, but that Defendants knowingly failed to employ adequate safeguards to protect their customers’ data, in violation of Defendants’ Privacy Policy.” *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *24. They also alleged that “Defendants’ knowing failure to employ adequate safeguards violated the policy of various California statutes, such as the [OPPA], that were intended to ‘reflect California’s public policy of protecting customer data.’” *Id.* (quoting *Anthem*, 162 F. Supp. 3d at 990).

Plaintiffs’ allegations here are not so detailed. *See, e.g.*, Compl. ¶¶ 13–14, 23. In their opposition, they argue that SNSC purposefully delayed notification to impacted users for no legitimate or law enforcement reason and failed to conduct a thorough investigation to adequately notify them about the results of any investigations. But the Complaint does not plead that there was a duty to provide timely breach notifications, or that SNSC breached such duty.

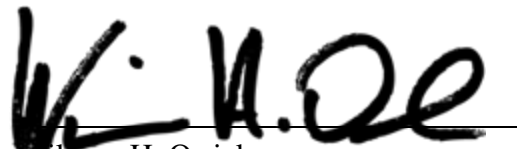
SNSC’s motion to dismiss the UCL claim under the unfair prong is GRANTED with leave to amend.

CONCLUSION

For the reasons discussed above, SNSC’s motion to dismiss is DENIED in part and GRANTED in part with leave to amend within twenty (20) days of this order.

IT IS SO ORDERED.

Dated: August 9, 2021



William H. Orrick
United States District Judge