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 GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: Dkt. No. 35

Plaintiff Desiree Schmitt brings 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, of which SNSC did not notify its customers for three months. SNSC has filed a motion to dismiss Schmitt's First Amended Complaint ("FAC"), which is GRANTED in part and DENIED in part, with leave to amend. The motion is GRANTED with prejudice on Schmitt's invasion of privacy claim because she has not adequately alleged egregious conduct by SNSC. The motion is also GRANTED on the claim brought under the "unlawful" prong of the UCL, with leave to amend. Although the Ninth Circuit permits the Federal Trade Commission ("FTC") Act and Guides to serve as predicates for unlawful UCL claims, Schmitt has not pleaded these violations with enough specificity. The motion is DENIED on Schmitt's claim brought under the "unfair" prong of the UCL as well as her negligence claim, as she has sufficiently pleaded elements of both.

BACKGROUND

Schmitt was a customer of SNSC, a financial services corporation that specializes in servicing residential, small balance commercial, consumer, and unsecured loans. FAC [Dkt. No. 34] ¶ 10. On or about October 15, 2020, a ransomware-threat group known as "Mount Locker"

(the "Unauthorized Party") deployed ransomware into SNSC's system and successfully acquired a number of digital files maintained by SNSC (known hereinafter as the "data breach"). *Id*. at ¶ 15. She states that the personal and financial information of at least 170,426 people were stolen and held for ransom. *Id*. at ¶ 18. She also alleges that despite learning of the data breach and alerting the Federal Bureau of Investigation "almost immediately," SNSC did not notify Schmitt or class members of the breach until January 14, 2021. *Id*. at ¶ 19.

SNSC's Notice of Data Breach ("Notice") informed recipients that personal information was acquired through a "ransomware" attack that "may include, but is potentially not limited to: your name, address, loan numbers, balance information and billing information such as charges assessed, owed and/or paid." *Id*. at ¶ 20 (citing Ex. B). The letter also stated that SNSC was "still in the process of conducting a comprehensive investigation of this incident" and that recipients "will be notified in the event we discover that any additional nonpublic personal information ('NPI') or personally identifiable information ('PII') pertaining to you was exposed." *Id*. at ¶ 21 (citing Ex. B). The Notice encouraged recipients, "[o]ut of an abundance of caution," to "remain vigilant . . . review your account statements and immediately report any suspicious activity." *See id*. at ¶ 67; Ex. B. It also recommended that recipients "obtain credit reports from each nationwide credit reporting agency." *Id*.

Schmitt claims that she did just that, purchasing credit monitoring at an annual cost of more than $200, along with a password manager (costing $3 per month) and password protection (costing more than $90). FAC at ¶ 68. She also contends that she has spent and will continue to spend "time and energy protecting and monitoring her identity and credit," including at least four hours reviewing bank accounts and statements and at least 10 hours changing "hundreds of passwords related to her business and personal accounts." *Id*. at ¶ 69.

This vigilance was warranted, Schmitt contends. She alleges that on or around July 16, 2021, SNSC provided a supplemental disclosure to some class members stating that names, contact information, birthdates, Social Security numbers, and "loan/borrower information" had also been stolen in the data breach. *Id*. at ¶ 30 (citing Ex. C). Schmitt concedes that she did not receive the July 16 letter, but notes that she had already filed this lawsuit when it was distributed.

Id. at ¶ 66. Schmitt further argues that she had "no reason to doubt, and every reason to assume," that her Social Security number, birthdate, and "loan/borrower information" was "also stolen and in the hands of criminals." *Id*. Schmitt asserts that she and other class members "provided their lenders, servicers, and SNSC with significant personal, income, and financial information that SNSC was able to acquire and to supplement by obtaining credit reports and banking information from third parties." *Id*. at ¶ 63. This information, she contends, includes: full names, mailing addresses, phone numbers, email addresses, loan identification numbers, tax information, and Social Security numbers. *See id*.

Schmitt contends that personal and financial information is "such a valuable commodity to identity thieves that once information has been compromised, criminals often trade the information on the 'cyber black-market' for years." *Id*. at ¶ 53. As such, she argues, "there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market," placing her and other class members "at an increased risk of fraud and identity theft for many years into the future." *Id*. at ¶ 54. She also alleges that after the data breach, she has experienced an "increase in spam, phishing attempts, and social engineering," including repeated robotexts to her cell phone. *Id*. at ¶ 70.

Schmitt blames SNSC for the data breach, arguing that its "failure to adhere to reasonable and necessary industry standards . . . resulted in the Data Breach and exacerbated its scope and impact." *Id*. at ¶ 32. She claims that SNSC undertook "basic steps recognized in the industry" to protect her and other class members' personal and financial information only after the breach. *Id*. at ¶ 35. According to Schmitt, these steps included "replacing email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence (AI) to detect and block known and newly introduced malware," and blocking all Internet traffic with foreign countries. *See id*. (citing Ex. B). Schmitt also alleges that SNSC failed to comply with FTC cybersecurity standards. *See id*. at ¶¶ 37-43. Schmitt argues that had SNSC properly maintained its systems and protected Schmitt and other class members' information, it could have prevented the breach. *See id*. at ¶ 44. She also contends that SNSC "should have notified all of its customers much sooner." *Id*. at ¶ 45.

Schmitt filed this lawsuit in San Francisco County Superior Court on March 12, 2021, bringing three claims on behalf of a nationwide class of borrowers impacted by the data breach: (1) negligence; (2) invasion of privacy; (3) the "unlawful" and "unfair" prongs of California's Unfair Competition Law ("UCL").[1] On May 5, 2021, SNSC removed the action to federal court and subsequently filed a motion to dismiss for failure to state a claim. Dkt. Nos. 1, 14. Although I found that Schmitt could assert California law claims as an Ohio resident, she failed to plausibly plead elements of those claims. *See* Mot. to Dismiss Order ("First MTD Order") [Dkt. No. 27] 1. As such, I denied the motion in part and granted in part with leave to amend. *Id*. Schmitt filed her FAC on August 30, 2021, which prompted a second motion to dismiss by SNSC. Dkt. Nos. 34, 35. I now consider that motion.

LEGAL STANDARD

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

In deciding whether the plaintiff has stated a claim upon which relief can be granted, the court accepts the plaintiff's allegations as true and draws all reasonable inferences in their favor. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact,

[1] A second plaintiff, James Furth, was named in the original complaint. *See* Dkt. No. 1. However, Furth was not named in the Amended Complaint, nor any of the filings related to this Motion to Dismiss.

or unreasonable inferences." *See In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

If the court dismisses the complaint, it "should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *See Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). In making this determination, the court should consider factors such as "the presence or absence of undue delay, bad faith, dilatory motive, repeated failure to cure deficiencies by previous amendments, undue prejudice to the opposing party and futility of the proposed amendment." *See Moore v. Kayport Package Express*, 885 F.2d 531, 538 (9th Cir. 1989).

DISCUSSION

I. INVASION OF PRIVACY

Under California law, a plaintiff must show three elements to adequately state a claim for invasion of privacy: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (internal citation omitted). SNSC again challenges the third element of Schmitt's claim.

There is a "high bar" for pleading an invasion of privacy claim. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012). "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an *egregious* breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 37 (1994) (emphasis added). "Even negligent conduct that leads to theft of highly personal information, including Social Security numbers, does not approach the standard of actionable conduct under the California Constitution and thus does not constitute a violation of plaintiffs' right to privacy." *iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (internal citation and quotation marks omitted).

SNSC argues that Schmitt again fails to allege any egregious or intentional conduct. Mot. to Dismiss ("MTD") [Dkt. No. 35] 6:11-12. Rather, SNSC contends, Schmitt makes "barebones allegations" that she has the right to be "highly offended" by the disclosure of her personal

information, and that the breach alone warrants proceeding with this claim. *Id*. at 6:11-15. SNSC argues that this does not amount to a serious invasion of privacy. *Id*. at 6:15. In support, SNSC cites two cases with similar allegations as those raised by Schmitt. In one, the court held that "[l]osing personal data through insufficient security doesn't rise to the level of an egregious breach of social norms underlying the protection of sensitive data like Social Security numbers." *Razuki v. Caliber Home Loans, Inc.*, No. 17-CV-1718, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018). In the other, the court dismissed an invasion of privacy claim because the plaintiff did not "allege any facts that would suggest that the data breach was an intentional violation of plaintiff's and other class members' privacy, as opposed to merely a negligent one." *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-CV-00014, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016).

These cases are more on point than the one cited by Schmitt, who argues that the instant circumstances are akin to the invasion of privacy that occurred in *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767 (N.D. Cal 2019). *See* Oppo. to Mot. to Dismiss ("Oppo.") [Dkt. No. 36] 16:19-20. *In re Facebook* arose from the Cambridge Analytica scandal, alleging that Facebook acted unlawfully by "making user information widely available to third parties" and "failing to do anything meaningful to prevent third parties from misusing the information they obtained." *Id*. at 777-78. According to Schmitt, "essentially the same conduct is alleged" here. Oppo. at 16:24.

It is difficult to see how Schmitt draws this conclusion. *In re Facebook* involved Facebook's alleged practice of intentionally sharing information about its users with a "non-exclusive list of business partners." *In re Facebook*, 402 F. Supp. 3d at 781. In turn, those companies allegedly shared data with Facebook. *Id*. In addition, Facebook was accused of doing nothing to stop those "business partners" from misusing the user information that Facebook provided. *Id*. In one instance—the Cambridge Analytica scandal that gave rise to the litigation—a researcher gave the information that he obtained from Facebook to a British consulting firm, which then used personal information from millions of Facebook accounts to send targeted political messages during the 2016 presidential campaign. *See id*. at 777.

That is a far cry from the allegations at hand. First, there is no indication of any intentional sharing of information by SNSC similar to that by Facebook. Schmitt does not contend that SNSC was in business with, purposefully shared consumers' personal information with, or received data from the Unauthorized Party. Schmitt claims that SNSC allowed access to consumers' personal information by storing it in "a place where hackers would target and easily succeed in acquiring it as a result of SNSC's unreasonable data security." Oppo. at 16:25-27 (citing FAC at ¶ 25, 111). But procuring information via security breach is inherently different than obtaining it through an agreed-upon exchange between business partners, as alleged in *In re Facebook*. *See In re Facebook*, 402 F. Supp. 3d at 781. Schmitt repeatedly refers to the incident involving SNSC as a "breach" and "attack," underscoring this crucial difference. *See, e.g.*, FAC at ¶ 1, 14, 23, 107.

Schmitt also cites *In re Facebook* in arguing that the "intimate details" regarding her and class members was sufficiently sensitive to render the data breach an invasion of privacy. Oppo. at 17:3-10. This argument also fails, as the compromise of any information resulted from alleged conduct that was (at most) negligent and not intentional. *See iPhone Application Litig.*, 844 F. Supp. 2d at 1063. ("Even negligent conduct that leads to theft of highly personal information, including Social Security numbers, does not . . . constitute a violation of plaintiffs' right to privacy.").

Because Schmitt has not met the high bar for pleading invasion of privacy, I GRANT SNSC's motion to dismiss the invasion of privacy claim with prejudice.

II. UCL

The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Civ. Code § 17200. Each prong provides a "separate and distinct theory of liability." *Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Schmitt claims violations of two of the three prongs, alleging unlawful and unfair actions by SNSC. *See* FAC at ¶¶ 115-122.

A. UNLAWFUL

The unlawful prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law." *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *23 (N.D. Cal. Aug. 30, 2017)

(citation omitted). "By proscribing 'any unlawful' business practice, the UCL permits injured consumers to 'borrow' violations of other laws and treat them as unlawful competition that is independently actionable." *Id*. However, the claim "must identify the particular section of the statute that was violated, and must describe with reasonable particularity the facts supporting the violation." *Bros. v. Hewlett-Packard Co.*, No. C-06-02254-RMW, 2006 WL 3093685, at *7 (N.D. Cal. Oct. 31, 2006) (internal citation omitted). If a plaintiff cannot state a claim under the "borrowed" law, he or she cannot state a UCL claim. *Golden v. Sound Inpatient Physicians Med. Grp., Inc.*, 93 F. Supp. 3d 1171, 1179 (E.D. Cal. 2015).

Schmitt alleges violations of the FTC Act and of FTC "regulations, guidance, and decisions" as grounds for her claim under the UCL's unlawful prong. FAC at ¶ 117 (citing in part 15 U.S.C. § 45, *et. seq*.). At oral argument, her counsel referenced a footnote in her brief that cited an electronic brochure published by the FTC, which was included in Schmitt's Opposition but not in her FAC. *See* Oppo. at 18 n.3.

I previously held that because the FTC Act did not confer a private right of action, it could not serve as a predicate for a UCL claim under the latter's unlawful prong. *See* First MTD Order at 16-17 ("For purposes of alleging an unlawful business practice, plaintiffs cannot predicate their UCL claim on the FTC Act."). I thought that *O'Donnell v. Bank of Am., Nat. Ass'n*, 504 Fed. Appx. 566 (2013) was more persuasive than the district court's ruling in *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953 (N.D. Cal. 2016), particularly because it came from the Ninth Circuit. *See* First MTD Order at 16-17.

Now, Schmitt cites new cases supporting her argument that the FTC Act and guidelines can provide the basis for an unlawful UCL claim, the most compelling of which come from the Ninth Circuit and the California Supreme Court. *See* Oppo. at 20. In *Rubenstein v. Neiman Marcus Grp. LLC*, 687 Fed. Appx. 564, 567 (9th Cir. 2017), the court held that "although the FTC Guides do not provide a private civil right of action, virtually any state, federal or local law can serve as the predicate for an action under the UCL." (internal quotation marks and citation omitted). Although this contradicts *O'Donnell*, it too directly addresses the lack of the private right of action as it pertains to FTC guidelines and the UCL and is later in time (though neither

case is precedential). It also aligns with the California Supreme Court's decision in *Rose v. Bank of America, N.A.*, 57 Cal. 4th 390, 397-98 (2013), which allowed UCL claims based on violations of the Truth in Savings Act, even though the statute's private right of action for damages had been repealed. For those reasons, I agree with the reasoning in *Rubenstein* and Schmitt may predicate her UCL unlawful claim on the FTC Act and FTC guidelines.

The problem, however, is that Schmitt again fails to plead violations of either the FTC Act or guidelines with the requisite particularity. When alleging unlawful conduct, the FAC predicates her UCL claim on violations of the FTC Act or FTC regulations, guidance, and decisions. *See* FAC at ¶ 117. But Schmitt does not name which specific provision of the FTC Act was allegedly violated, let alone how. *See id*. The same goes for the FTC guidelines. Unlike in *Rubenstein*, where the plaintiffs alleged violations of specific FTC Guides (the Guides Against Deceptive Pricing, 16 Code of Federal Regulations Sections 233.1 and 233.2(c)), Schmitt only mentions general FTC "guides" and "standards." *See Rubenstein*, 687 Fed. Appx. at 566; FAC at ¶¶ 37-38, 117.

The footnote counsel mentioned does not save the claim. It cites an electronic "guide for business" published by the FTC. *See* Oppo. at 18 n.3 (linking to "Protecting Personal Information: A Guide for Business"). But the authority of this document is unclear. It does not appear to cite to any federal regulations, as in *Rubenstein*. *See id*. It encourages readers to "take stock of the law" and references three statutes that "may require you to provide reasonable security for sensitive information," but does not elaborate beyond providing a link to the FTC website. *See id*. at 6. Moreover, the introduction to the document describes it as a "brochure." *Id*. at 2. There is no indication that this document constitutes a law or federal regulation, nor carries the weight of such. Without any argument from Schmitt showing this, this document cannot serve as a predicate for her unlawful UCL claim.

Schmitt also points to a Third Circuit case as well as SNSC's Privacy Policy in arguing that her allegations have the requisite particularity. *See* Oppo. at 18-19. But neither resolve the ongoing flaw in the pleadings: Schmitt has failed to (1) identify a particular section of the statute (in this case, the specific provision of the FTC Act or an FTC Guide); and (2) describe with any

particularity the facts supporting the purported violations of that section.

Accordingly, I find that Schmitt has not adequately pleaded a violation of a statute giving rise to a claim under the unlawful prong of the UCL.

B. UNFAIR

The unfair prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by another law. *In re Yahoo!*, 2017 WL 3727318, at *23 (citation omitted). The UCL does not define "unfair," and the "proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." *Id*. Some courts apply what is referred to as the "tethering test," where unfairness must "be tethered to some legislatively declared policy or proof of some actual or threatened impact on competition." *Lozano*, 504 F.3d at 735 (citation omitted). Others use the "balancing test," which requires courts to "weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (internal quotation marks omitted). 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." *In re Anthem*, 162 F. Supp. 3d at 990.

SNSC contends that Schmitt fails both tests. First, SNSC asserts that because Schmitt has failed to allege "any legitimate violation of statutory law, there is no legislative policy" to which she can tether her claim. *See* MTD at 11:10-18. SNSC extends this argument to the first aspect of the balancing test, again asserting that Schmitt cannot show that SNSC violated an "clear, established public policy." *Id*. at 12:22-13:12. Regarding the second aspect of the balancing test, SNSC asserts that Schmitt has not alleged how the ransomware attack amounts to "immoral, unethical, oppressive, unscrupulous or substantially injurious" acts, beyond "reciting the words" in the FAC. *See id*. at 12:14-17.

Turning first to the tethering test, I agree that Schmitt has not sufficiently pleaded a

violation of public policy.[2] The FAC contends that it is the "established public policy of this state that confidential information entrusted to financial institutions . . . be adequately protected from outside institutions." FAC at ¶ 116. Schmitt also alleges that "SNSC's practices were contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal and financial data utilize appropriate security measures." *Id.*

Schmitt argues that these public policies are reflected in the FTC Act, Section 1798.81.5 of the California Civil Code, and Article I, Section 1 of the California Constitution. *See id.* But the FTC Act and cited section of the California Constitution make no mention of personal information or consumer data, nor the legislative intent behind either. *Cf. In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1227 (N.D. Cal. 2014) (noting that "California legislative intent is clear" as to the cited statutes, allowing plaintiffs to adequately allege a claim under the UCL's unfair prong); *Diva Limousine, Ltd. v. Uber Techs., Inc.*, 392 F. Supp. 3d. 1074, 1091 (N.D. Cal. 2019) (finding that plaintiffs adequately alleged an unfair UCL claim because the California Labor Code "expressly declares that 'it is the policy of this state to vigorously enforce minimum labor standards'" relevant to the claim). These provisions might in fact reflect the public policy that Schmitt alleges. But she needs to draw a more direct line between the two in order to adequately allege that SNSC's actions violated any public policy.

Section 1798.81.5(a)(1) of the California Civil Code expressly declares the Legislature's intent to protect personal information. As I have previously stated, however, case law indicates that this section only applies to California residents, suggesting that any associated public policy may be similarly limited. *See* First MTD Order at 17 (citing *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012); *see also* Cal. Civ. Code § 1798.81.5(a)(1) ("It is the intent of the Legislature to ensure that personal information *about California residents* is protected.") (emphasis added). Schmitt does not argue otherwise.

That said, I find that Schmitt has plausibly alleged "immoral, unethical, oppressive,

[2] Schmitt did not allege any actual or threatened impact on competition by SNSC. *See* FAC at ¶¶ 116-122.

unscrupulous or substantially injurious" conduct by defendants, satisfying the balancing test at this stage of the litigation. *In re Anthem*, 162 F. Supp. 3d at 990. The FAC offers sufficient facts to allege this type of conduct, in part by claiming that SNSC represented in its Privacy Policy that "to protect . . . personal information from unauthorized access and use" it used security measures including "computer safeguards, secured files and buildings," but knowingly failed to employ adequate safeguards. *See* FAC at ¶ 119; Ex. A. While I agree with SNSC that its own Privacy Policy does not carry the same weight as a legislatively declared public policy, the key is that SNSC represented to customers that it would protect their personal information despite knowing, according to Schmitt, that it had inadequate safeguards in place. *See* Reply [Dkt. No. 37] 5:25-27. Moreover, Schmitt alleges that SNSC's conduct was "immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious" when it failed to disclose the data breach in a timely manner, now pleading that SNSC had a duty to so. *See, e.g.*, FAC at ¶ 118. Therefore, based on the balancing test, I find that Schmitt has sufficiently stated a claim under the unfair prong of the UCL.

For these reasons, SNSC's motion to dismiss is DENIED with respect to the claim brought under the unfair prong of the UCL. It is GRANTED on the claim brought under the unlawful prong, with leave to amend.

III. NEGLIGENCE

To state a claim for negligence in California, a plaintiff must show duty, breach, causation, and damages. *Conroy v. Regents of Univ. of Cal.*, 45 Cal. 4th 1244, 1250 (2009).

A. PERSONAL IDENTIFYING INFORMATION

As an initial matter, in my prior Order, I held that Schmitt failed to adequately assert that personal identifying information ("PII") was among the information compromised during the data breach—and thus, could not show that SNSC had a duty to protect that information. First MTD Order at 8:16-19. I stated that Schmitt could show this by "pleading what kind of information [she], and customers like [her], provided to SNSC." *Id*. at 8:19-20. "With allegations that certain less sensitive information was released during the data breach . . . and that SNSC at least had in its possession other more sensitive information (which rise to the level of PII), a reasonable inference

could be drawn that PII was also among the information compromised." *Id*. at 8:20-24.

SNSC asserts that Schmitt has again failed to do this. *See* MTD at 14. SNSC relies heavily on the language of the Notice sent to customers, which it argues makes "abundantly clear that plaintiff has no case because none of her PII was accessed and compromised." *Id*. at 14:11-16. SNSC cites excerpts, including:

- SNSC is "not aware of the misuse of any of your information. . . ."
- "[N]one of the information that was compromised included credit card information, or banking account information. . . ."
- "The information compromised was largely limited to March 2018 Billing Statements and fee notices. . . ."
- "[Y]ou will be notified in the event we discover that any . . . personally identifiable information ('PII') pertaining to you was exposed."

Id. at 14 (citing FAC, Ex. B).

Schmitt responds by arguing that she adequately amended her Complaint to include the types of information about Schmitt and class members that SNSC possessed at the time of the breach. *See* Oppo. at 7:11-18. She first cites SNSC's Privacy Policy, which states that SNSC collects and shares information that can include Social Security numbers and account balances, transaction and credit histories, credit scores, and mortgage rates and payments. *See* Oppo. at 7:12-15 (citing FAC at ¶ 12). Schmitt adds to this list later in the FAC, alleging that she and class members "provided their lenders, servicers, and SNSC with significant personal, income, and financial information that SNSC was able to acquire and to supplement by obtaining credit reports and banking information from third parties." *Id*. at ¶ 63. That information, Schmitt asserts, includes Social Security numbers, full names, property and insurance details, loan history information, and tax and credit information. *See id*.

In deciding whether a plaintiff has stated a claim upon which relief can be granted, I must accept her allegations as true and draw all reasonable inferences in her favor. *See Usher*, 828 F.2d at 561. California law recognizes the disclosure of a person's name and Social Security number as the disclosure of PII. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(i). Schmitt proffers enough factual allegations—including SNSC's own Privacy Policy—to reasonably infer that SNSC had Social

Security numbers in its possession when the breach occurred. *See* FAC at ¶¶ 12, 63. This allegation is also supported by the supplemental disclosure sent to class members, stating that the Unauthorized Party "may have had access" to names, contact information, birthdates, Social Security numbers, and "loan/borrower information" during the data breach. *Id*. at ¶ 30 (citing Ex. C). Although Schmitt did not receive the letter, she notes that this lawsuit was pending at the time it was distributed. *Id*. at ¶ 66. Drawing all reasonable inferences in her favor, I find that Schmitt has sufficiently pleaded that the information compromised in the data breach included PII.

B. DUTY OF CARE

California courts consider several factors when determining the existence of a legal duty. The "*Rowland* factors" include: (1) the foreseeability of harm to the plaintiff; (2) the degree of certainty that the plaintiff suffered injury; (3) the closeness of the connection between the defendant's conduct and the injury suffered; (4) the moral blame attached to the defendant's conduct; (5) the policy of preventing future harm; (6) the extent of the burden to the defendant and consequences to the community of imposing a duty; and (7) the availability, cost, and prevalence of insurance for the risk involved. *Regents of Univ. of Cal. v. Superior Court*, 4 Cal. 5th 607, 628 (2018). The *Regents* court noted that these factors fall into two categories: one involving "foreseeability and the related concepts of certainty and the connection between plaintiff and defendant," and the other examining "public policy concerns of moral blame, preventing future harm, burden, and insurance availability." *Id*. at 629. The court also noted that the factors "must be evaluated at a relatively broad level of factual generality." *Id*. at 628.

i. Foreseeability Factors

SNSC argues that the first *Rowland* factor is not met because Schmitt's alleged harm—"expenses and/or time spent on credit monitoring"—was not foreseeable. MTD at 15:14-16 (citing FAC at ¶ 109). SNSC describes the Schmitt's actions as "entirely unnecessary" and "voluntary," arguing that because her PII was not accessed or misused, there was no need for her to spend time or money monitoring her credit. *See id*. at 15:16-24. SNSC cites the Notice as affirming that Schmitt's PII was not accessed or misused, along with the supplemental disclosure in arguing that SNSC offered "complimentary credit monitoring and identity theft services" to

affected individuals. *Id*. at 15:18-26 (citing FAC, Exs. B, C). The latter, SNSC argues, further shows there was "no reason to incur this 'harm.'" *Id*. at 15:19.

As Schmitt argues, this ignores the language of the Notice itself. *See* Oppo. at 10:26-11:9. In the letter, SNSC encouraged recipients to "remain vigilant over [the] next twelve (12) to twenty-four (24) months, review your account statements and immediately report any suspicious activity." *See* FAC, Ex. B. It also recommended that recipients "regularly obtain credit reports from each nationwide credit reporting agency." *Id*. SNSC's argument that its own recommendations were not foreseeable is not persuasive.

SNSC summarily challenges the second and third *Rowland* factors—the degree of certainty that Schmitt suffered injury and closeness of the connection between SNSC's conduct and the alleged injury—on the same grounds. *See* MTD at 16:1-7. However, as explained below, the money and time Schmitt spent monitoring her credit constitutes a sufficient injury for her claims to proceed. She also adequately alleges that her injury is closely connected to SNSC's purported failure to protect the personal information of Schmitt and other class members, along with its recommendation that customers monitor their credit. *See* Oppo. at 11:18-24.

ii. Policy Factors

Turning to the policy-related factors, SNSC first argues that there is "no moral blame to attach to SNSC," particularly when the ransomware attack and purported harm to Schmitt was not foreseeable. *See* MTD at 16:9-11. In support, SNSC cites *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *6 (N.D. Cal. Sept. 14, 2016), which analyzed moral blameworthiness under the economic loss doctrine. In *Castillo*, the court held that the plaintiffs failed to adequately plead that the defendant's actions were immoral because they had not "provided enough information to permit an inference that [the defendant] should have been on the lookout for fraudulent requests for W-2 information." *See id*. Without "reckless or purposeful behavior," SNSC argues, "no moral blame can attach." *See* MTD at 16:17-18 (citing *Castillo*, 2016 WL 9280242, at *6).

But *Castillo* is distinguishable. The *Castillo* plaintiffs alleged that the defendant owed them a duty to "protect their personal identifying information and to inform them reasonably

promptly about the phishing attack." *See Castillo*, 2016 WL 9280242, at *2. Schmitt takes issue with SNSC's purported misrepresentations in its Privacy Policy, along with the delayed notification to customers after the data breach was discovered. Oppo. at 11-12; *see also* FAC at ¶ 105-106 (alleging "reckless disregard" by SNSC). And while the *Castillo* plaintiff were informed of the breach either "a few days" or "about a week" after it occurred, Schmitt alleges she was not notified for three months. *See Castillo*, 2016 WL 9280242, at *1; FAC at ¶ 19.

I also find that the policy of preventing future harm favors imposing a duty of care, as it would strengthen information security for customers like Schmitt, who entrust companies like SNSC with their PII and, in the event that something goes awry, expect prompt notification. *See* Oppo. at 12-13. Again, SNSC cites a distinguishable case when arguing otherwise. *See* MTD at 16:26-17:6. It is true that the court in *Sakai v. Massco Invs., LLC*, 20 Cal. App. 5th 1178, 1189-90 (2018), declined to find liability for harm caused by a third party "as a matter of policy," citing in part the "onerous" burden of implementing preventative measures. But that case involved markedly different circumstances, arising after a taco truck customer was struck by a vehicle in a gas station parking lot. *See id*. at 1181-82. Any burden imposed on SNSC to strengthen its security measures or speed up its notification processes would be incurred by a large company, not the owner of a gas station. *See* MTD at 17:7-15. The benefits would also reach a wider audience. Schmitt has adequately alleged that any burden would be outweighed by the "significant" benefits of reducing "identity fraud, phishing, and social engineering schemes," as well as lessening the risks of customers' identity theft and fraud. *See* Oppo. at 13:7-15. Although the parties disagree as to the expense and availability of insurance, the final *Rowland* factor, it is not dispositive, as the remaining factors all weigh in favor of imposing a duty of case.

For these reasons, I find that Schmitt has adequately alleged that SNSC had a duty of care to protect her PII.[3]

[3] Schmitt also contends in her Opposition that SNSC had a duty of case based on a special relationship, because it created the peril, and under the doctrine of negligence per se. *See* Oppo. at 8-9. Because I find that Schmitt has adequately pleaded a duty of care under the *Rowland* factors, I need not evaluate the duty in these other contexts.

C. BREACH

SNSC does not challenge breach in its Motion to Dismiss. I previously noted that if Schmitt were to adequately allege a plausible legal duty, the burden to plead a corresponding breach based on SNSC's inadequate security measures was "not high." *See* First MTD Order at 8:26-28. Because Schmitt has adequately alleged a duty, I see no issue with breach.

D. CAUSATION AND DAMAGES

SNSC challenges causation and damages with familiar arguments. It argues that Schmitt "does not make the requisite connection between the alleged breach and [her] damages" because she does not assert that: "(1) her PII was actually stolen and misused, (2) she was a victim of identity theft or fraud, and (3) she did not suffer identify theft or fraud prior to this incident." *See* MTD at 18:15-18.

These arguments have been settled. As stated in my prior Order, recent case law makes clear that "time and money" a plaintiff spends on credit monitoring in response to a data breach "is cognizable harm to support [a] negligence claim." *See* First MTD Order at 10 (citing *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 649-50 (N.D. Cal 2020) and other cases). Schmitt has clearly asserted plausible damages under existing law.

In my prior Order, I also noted that if Schmitt were to plausibly plead that her PII was compromised, "a reasonable inference would follow that [her] decision to purchase monitoring services was 'reasonable' and 'necessary.'" *See* First MTD Order at 12:1-2. As explained above, Schmitt has done this. Again, I see no reason to depart from my earlier thinking.

Given these considerations, I find that Schmitt has sufficiently pleaded a claim for negligence. Accordingly, SNSC's motion is DENIED on this claim.

CONCLUSION

For the foregoing reasons, SNSC's Motion to Dismiss is GRANTED in part and DENIED in part, with leave to amend in twenty days.

IT IS SO ORDERED.

Dated: November 12, 2021

William H. Orrick
United States District Judge