UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JASEN SILVER ET AL.,

Plaintiffs,

v.

STRIPE INC.,

Defendant.

Case No. 4:20-cv-08196-YGR

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' AMENDED COMPLAINT

Re: Dkt. No. 48

Plaintiffs Jasen Silver, Jill Lienhard, Patricia Tysinger, Victoria Waters, and Alaina Jones bring this amended class action complaint against defendant Stripe Inc. ("Stripe") alleging violations of various privacy laws. (Dkt. No. 47.) ("First Amended Complaint" or "FAC.") Plaintiffs assert nine causes of action: (1) violation of the California Invasion of Privacy Act ("CIPA") under California Penal Code § 631; (2) violation of CIPA under California Penal Code § 635; (3) violation of the Florida Security of Communications Act ("FSCA"), Florida Statutes § 934; (4) violation of Washington's Wiretap Act, Revised Code of Washington § 9.73.030; (5) violation of the Utah Notice of Intent to Sell Nonpublic Personal Information Act, Utah Code Ann. § 13-37-201; (6) invasion of privacy under California's constitution; (7) intrusion upon seclusion (California); (8) violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq.; and (9) unjust enrichment.

Having once considered a motion to dismiss, now before the Court is Stripe's motion to dismiss all causes of action of the revised First Amended Complaint. (Dkt. Nos. 47 and 48.) The matter was fully briefed by the parties. (*See also* Dkt. Nos. 51 and 53.)

The Court has carefully considered the papers submitted, the pleadings in this action, oral argument, and for the reasons set forth below, it **GRANTS IN PART AND DENIES IN PART** the

motion to dismiss plaintiffs' first amended complaint.[1]

I. BACKGROUND

The First Amended Complaint alleges as follows:

Stripe violated various privacy laws by secretly tracking, collecting, and storing the personal data and web activity of visitors to merchants' website. (FAC ¶¶ 1, 206.) It then created Stripe Elements, a software code that allows merchants to integrate Stripe's payment platform into their applications. (*Id.* ¶ 3.) Merchants that use Stripe Elements, in this case Instacart, as a payment platform do not usually contain any identifying information or identification to alert consumers that their transactions are being processed by Stripe. (*Id.* ¶ 4.) Specifically, there is no branding on the payment screens indicating that Stripe is involved, and other than by looking into the detailed coding of the website and the platform, consumers cannot tell that Stripe is obtaining or storing sensitive information, including financial information. (*Id.* ¶¶ 4-6.)

Consequently, most users think that they are communicating directly with the merchant, when they are in fact communicating directly with Stripe. (*Id.*) In addition to sensitive financial information, Stripe collects, stores, and uses the following information:

- the consumer's mouse movements and clicks;
- the consumer's keystrokes;
- the consumer's IP address and internet service provider;
- the geolocation of the consumer and his or her device;
- the consumer's device brand and model, browser, and operating system;
- the number of cards that have been used at the consumer's IP address;
- the number of declined cards the consumer had used with Stripe;
- a record of when the consumer's attempted purchases were declined;
- the name of the consumer's bank or card issuer;
- whether or not the consumer had sufficient funds for the transaction;

[1] The parties do not dispute the legal standard for a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). The Court applies the well-accepted principles articulated by the parties.

- the time of day the consumer makes the purchase;
- other processing codes returned by the consumer's bank, such as "do not honor" codes or those relating to stolen cards; and
- whether the consumer later disputes the charge.

("at-issue data") (*Id*. ¶¶ 7, 36.)

Stripe takes all the collected information, correlates all payments the consumer made across its entire platform, and then—without informing the consumer—provides much of it to its other merchants. (*Id*. ¶ 9.)

Next, Stripe installs cookies on consumers' computers and mobile devices, "so that Stripe can track their purchasing behavior across its vast merchant network." (*Id*. ¶ 8.) For example, merchants are able to view a consumer's history of transactions processed by Stripe. (*Id*.) Using this history, Stripe makes what is known as a "Risk Insights," which assigns a risk score to each consumer's transactions based on numerous factors. (*Id*. ¶ 10.) At no time does Stripe inform consumers who use Stripe Elements that any of the alleged conduct is taking place. (*Id*. ¶ 12.)

A. Content of the Privacy Policy

Relevant here, the privacy policy contains three provisions. First it states that Instacart may share "information about you and your order with ***the other parties*** who help enable the service" and that "[t]his includes . . . the ***payment processing partner(s)*** that we use to validate and charge your credit card. . . ." No one disputes that Stripe is a payment processing partner. (Dkt. No. 22) (Declaration of Jonathan H. Blavin ("Blavin Decl."), Ex. C at 3-4, § IV (emphases supplied.)) Second, it states that Instacart may "disclose the following categories of personal information ***to third parties*** for our commercial purposes: identifiers, demographic information, commercial information, relevant order information, internet activity, geolocation data, sensory information, and inferences." (*Id*. at 5, § VIII (emphasis supplied); *id*. at 1-3, § II; 3-4, § IV.) Third, the privacy policy expressly provides:

> We, ***our partners***, our advertisers, and third-party advertising networks ***use various technologies to collect information***, including but not limited to cookies, pixels, scripts, and device identifiers. . . .

> ***Our partners***, advertisers, and third-party advertising networks ***may use these technologies to collect information about your online activity*** over time and across different websites or online services.

(Blavin Decl., Ex. C at 2, § II (emphases supplied.))

II. ANALYSIS

A. Consideration of Consent is Appropriate

Consideration of consent is appropriate on a motion to dismiss where lack of consent is an element of the claim. *E.g. Garcia v. Enter Holdings, Inc.*, 78 F. Supp. 3d 1125, 1136 (N.D. Cal. 2015) ("[d]efendants may properly challenge [p]laintiffs's allegations regarding lack of consent through the instant motion to dismiss); *Javier v. Assurance IQ, LLC,* No. 4:20-CV-02860-JSW, 2021 WL 940319, at *2 (N.D. Cal. Mar. 9, 2021) (explaining that "consent generally defeats privacy claims" and granting motion to dismiss); *Smith v. Facebook, Inc.*, 745 F.App'x, 8, 9 (9th Cir. 2018) (affirming motion to dismiss based on consent).

Plaintiffs' first four causes of action depend on consent. With respect to plaintiffs' first and second causes of action, Cal. Penal Code Section 631(a) prohibits wiretapping "without the consent of all parties to the communication," and Cal. Penal Code. Section 635 also depends on consent. *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (user consent is a defense under CIPA); *see also Cramer v. Consol. Freightways, Inc*., 209 F.3d 1122, 1130, n.9 (9th Cir. 2000) (*amended on other grounds* 255 F.3d 683 (9th Cir. 2001)) (explaining that a claim under Cal. Penal Code "Section 635 requires proof that the plaintiff was "injured' by the eavesdropping equipment, which in turn also depends on consent"). Similarly, plaintiffs' third and fourth causes of action under the FSCA and Washington's Wiretap Act both require lack of consent. *See* Fla. Stat. Ann. § 934.03(2)(d) (permits interception of a communication "when all of the parties to the communication have given prior consent"); Wash. Rev. Code Ann. §§ 9.73.030(1) (a)-(b) (permits interception with "the consent of all the participants"). Thus, the Court's consideration of consent as to plaintiffs' first, second, third, and fourth causes of action is appropriate here.

B. Online Consent of Privacy Policy

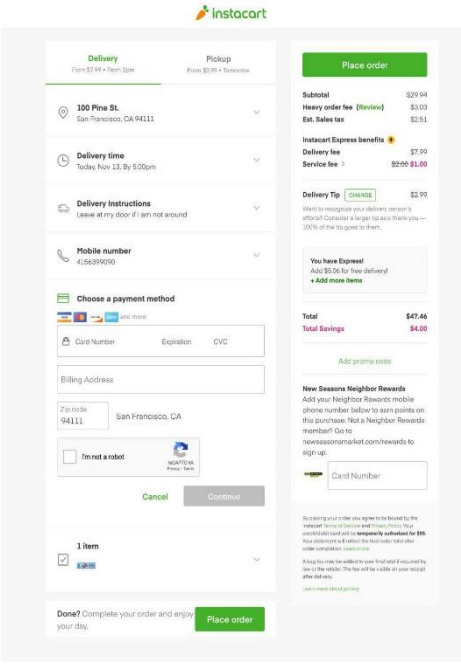
Internet users can form online contract, and therefore consent, in a variety of ways. *See Colgate v. JUUL Labs, Inc.*, 402 F. Supp. 3d 728, 763 (N.D. Cal. 2019) (discussing different forms of online contracts). The Ninth Circuit recognizes three main types of contracts formed on the internet: "clickwrap", "browsewrap", and "sign-in wrap" agreements. "Clickwrap" agreements require website users to click on an "I agree" box after they are presented with a list of terms and conditions. *Id.* "Browsewrap" agreements do not require the express consent, but instead operate by placing a hyperlink with the governing terms and conditions at the bottom of the website. *Id.* In "browsewrap" agreements, a user gives consent just by using the website. *Id.* "Sign-in-wrap" agreements are those that present a screen that states that acceptance of a separate agreement is required before a user can access an internet product or service. *Id.*

The Ninth Circuit requires that online contracts put a website user on actual or inquiry notice of its terms. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014). In doing so, the notice must be conspicuous, that is it must put "a reasonably prudent user on inquiry notice of the contracts." *Id.* Whether a user has such inquiry notice "depends on the design and content of the website and the agreement's webpage." *Id.*

Courts have found that "[a] binding contract is created if a plaintiff is provided with an opportunity to review the terms of service in the form of a hyperlink," and it is "sufficient to require a user to affirmatively accept the terms, even if the terms are not presented on the same page as the acceptance button as long as the user has access to the terms of service." *Moretti v. Hertz Corp.*, No. C 13–02972 JSW, 2014 WL 1410432, at *2 (N.D. Cal. Apr. 11, 2014); *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1166 (N.D. Cal. 2016) (user agreement enforceable where user had to "take some action— a click of a dual-purpose box— from which assent might be inferred").

Here, no dispute exists that Instacart utilized a "sign-in wrap" agreement. Instacart's purchase checkout page required plaintiffs to agree to Instacart's terms of service and privacy policy whenever they placed an order. Plaintiffs admit that they were presented with the checkout screen as they completed their Instacart orders. (FAC ¶¶ 59, 72, 84, 97, 110.) Instacart's

checkout page is depicted below:



(*See* FAC, ¶ 30, Fig. 2.)

The Court finds Instacart's privacy policy conspicuous and obvious for several reasons. First, the hyperlink to the privacy policy is displayed in a bright green font against a white background, which stands out from most of the surrounding text. Further, the hyperlink to the privacy policy is located close to the "place order" button, thus it is hard for a user placing an order to miss it. The bold font alerting consumers to the amount of the charge hold placed on their card calls additional attention to the area where Instacart's privacy policy is located. There is nothing about the text that makes it inconspicuous or nonobvious.

The Court finds that a reasonably prudent user would have been aware of Instacart's privacy policy when placing an order. This finding comports with other courts that have found similar "sign-in wrap" agreements to be valid *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 75-76 (2d. Cir. 2017) ("the existence of the terms was reasonably communicated to the user") (collecting cases); *see also Peter v. DoorDash, Inc.*, 445 F. Supp. 3d 580, 587 (N.D. Cal. 2020). Based thereon, the Court finds that during checkout, plaintiffs were "provided with an opportunity to review the terms" of the privacy policy. *Crawford v. Beachbody, LLC*, No. 14cv1583–GPC(KSC), 2014 WL 6606563, at *3 (S.D. Cal. Nov. 5, 2014). They were required to take an

affirmative step—clicking the "Place Order" button—to acknowledge that they were agreeing to the terms of the privacy policy. They were told the consequences that would follow from clicking the button, including their acceptance of the privacy policy. Plaintiffs decided to place an order after being made aware of the privacy policy. Accordingly, the Court finds that plaintiffs consented to Instacart's privacy policy each time they placed an order. *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d at 1166.

C. Wiretap Claims: First, Second, Third, and Fourth Causes of Action

Next, the Court considers whether plaintiffs' consent to the policy defeat their wiretap claims. Courts consistently hold that terms of service and privacy policies, like Instacart's privacy policy here, can establish consent to the alleged conduct challenged under various states wiretapping statutes and related claims. *See Smith*, 745 F. App'x 8 (consent established for wiretapping claims given that "[t]erms and [p]olicies contain numerous disclosures related to information collection on third-party websites"); *Garcia*, 78 F. Supp. 3d at 1135–37 (dismissing CIPA claim where app provider's terms and privacy policy provided consent for the alleged disclosures).

Plaintiffs claim that the policy does not provide sufficient notice that Stripe would collect the information that it did. However, there are provisions that disclose that third parties like Stripe may obtain not only credit card data, but also "identifiers, demographic information, commercial information, relevant order information, internet activity, geolocation data, sensory information, and inferences." (Blavin Decl., Ex. C at 5, § VIII; 1–3; § II; 3–4, § IV.) There are also provisions that disclose that Instacart's "partners"—again without limitation—"use various technologies" to "collect information about your online activity over time and across different websites or online services." (*Id*. at 2, § II.) These terms plainly disclose that partners like Stripe may install tracking software to collect data concerning users' activities across websites. That the disclosures were provided by Instacart (as opposed to Stripe directly) does not require a different result. *E.g.*, *Perkins v. LinkedIn Corp*., 53 F. Supp. 3d 1190, 1213 (N.D. Cal. 2014) (finding that LinkedIn user consented as a matter of law to conduct based on statements made by third party Google); *see also Javier*, 2021 WL 940319, at *2 (holding that consent to the conduct of a third-party partner can be

established via a website's disclosures). Instacart's privacy policy explicitly states that consumers' information may be provided to its "partners."

Instacart's use of the word "may," as opposed to "will," in the privacy policy does not make it such that the policy gives insufficient notice of the alleged conduct. Privacy policies often make disclosures by stating what companies "may" do, and such disclosures have been upheld time and again by courts as sufficient to establish consent. *E.g.*, *Cooper v. Slice Techs., Inc.*, No. 17-cv-7102, 2018 WL 2727888, at *4 (S.D.N.Y. June 6, 2018) ("Plaintiffs argue that the privacy policy is misleading because it says only that UnrollMe may sell consumer data, not that it would do so. But this distinction is without difference. If I ask you if I may enter your house, and you say yes, you have given me permission to enter your house."); *Javier*, 2021 WL 940319, at *4 (rejecting argument that privacy policy states that "Assurance 'may' use third party monitors" as "policy clearly indicates that Assurance tracks activity on its website and may use third party vendors to do so"); *Garcia*, 78 F. Supp. 3d at 1136 ("The Privacy Policy expressly states that 'we may share your personal information with our . . . service provider'"); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 792–93 (N.D. Cal. 2019) (terms "flagged for users the possibility that other people 'may share' their information 'with applications'").

Plaintiffs' one cited case, *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013), standing for the proposition that the word "may" is too indefinite, is oversimplified. There, the court held that the alleged conduct—Google's reading of emails to send targeted advertisements—was not adequately disclosed in its terms stating that "advertisements may be targeted to the content of information *stored* on the Services, queries made through the Services or other information." *Id.* at *13. In so holding, the court cited several reasons, including that the language only suggested that stored information was accessed and not "in transit via email". The court also found that the policy suggested that "any consent" to intercept emails was "only for the purpose" of "eliminat[ing] objectionable content". *Id.* The mere inclusion of the word "may" was therefore not dispositive to the court's holding that the disclosure was inadequate. *Id.* By contrast, the privacy policy here clearly discloses the challenged conduct—that third parties like Stripe may collect and use a consumer's sensitive data,

including one's financial information and web activity.

Thus, the Court finds that plaintiffs consented to the collection of the data at-issue. Accordingly, the Court **GRANTS** the motion to dismiss as to plaintiffs' wiretap claims (first, second, third, and fourth causes of action) based on plaintiffs' consent to the collection of the data.

D. Utah's Notice of Intent to Sell Nonpublic Personal Information: Fifth Cause of Action

Under Utah's Notice of Intent to Sell Nonpublic Personal Information Act, a commercial entity that enters into a "consumer transaction" with a consumer must give notice to the consumer before the entity discloses nonpublic information to a third-party. Utah Code Ann. § 13-37-201(1). The statute defines a "consumer transaction" as "the use of nonpublic personal information in relation to a transaction with a person if the transaction is for primarily personal, family, or household purpose." *Id.* § 13-37-102(4).

The Court finds that the complaint, on its face, sufficiently alleges a claim under Utah's statute. Plaintiffs allege that Stripe qualifies as a business entity under the statute because Stripe conducts business in Utah. Further, the complaint sufficiently alleges that Stripe conducted "consumer transactions" with plaintiffs. For instance, the complaint alleges that Stripe collected plaintiffs' personal information while they used Instacart to shop for "personal, family and household purposes." In return, as alleged, Stripe then processed plaintiffs' payment, allowing plaintiffs to complete the transaction. The Court finds that the complaint alleges sufficient facts to state a claim under the statute.

However, class action relief is unavailable under the statute. Section 13-37-203(3) provides that "a person may not bring a class action" for violation of the statute. Utah Code Ann. § 13-37-203(3). Thus, the Court **DENIES** the motion to dismiss as to Ms. Alaina Jones individually, the Utah resident named in the complaint, but **GRANTS** the motion as to the Utah Class.

E. Invasion of Privacy and Intrusion Upon Seclusion: Sixth and Seventh Causes of Action

To state a claim for invasion of privacy under the California Constitution, a plaintiff must plead: (1) they possess a legally protected privacy interest, (2) they maintain a reasonable

expectation of privacy, and (3) the intrusion is highly offensive. *Hernandez v. Hillsides, Inc.*, 47 Cal 4th 272, 287 (2009).

A claim for intrusion upon seclusion under California common law involves similar elements. Plaintiffs must show that: (1) a defendant "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy," and (2) that the intrusion was "highly offensive" to a reasonable person. *Id.* at 286.

Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exist a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *See In re Facebook, Inc., Internet Tracking Litig.*, 956 F. 3d 589, 605 (9th Cir. 2020). However, whether a conduct was highly offensive cannot be resolved at the pleading stage. *Id.* at 606.

Thus, the relevant question here is whether plaintiffs would reasonably expect that a third party such as Stripe would disclose plaintiffs' data to other third parties.[2] Plaintiffs argue that Instacart's policy does not disclose Stripe's disclosure activities. Specifically, plaintiffs claim that the policy does not disclose that Stripe would use their data to create and share risk profiles with their merchants.

Stripe relies on the following notice in Instacart's policy to argue that there is proper notice of Stripe's disclosure practice:

> We may share your information when we believe that the disclosure is reasonably necessary to (a) comply with applicable laws, regulations, legal process, or requests from law enforcement or regulatory authorities, (b) prevent, detect, or otherwise handle fraud, security, or technical issues, and (c) protect the safety, rights, or property of any person, the public, or Instacart.

Blavin Decl., Ex. C at 4, § IV.

While plaintiffs initially consented to the Stripe's initial collection of the at-issue data, that consent is not unlimited. Privacy is not an "all-or-nothing" proposition. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767 at 782. The complaint sufficiently

[2] Having already found that plaintiffs consented to the collection of the at-issue data, the Court's remaining analysis only focuses on Stripe's disclosure of the information.

alleges that plaintiffs did not consent to Stripe's disclosure of their information to Stripe's merchants and customers. For instance, plaintiffs allege that Stripe does not inform Instacart users that it, a third party itself, would further disclose the at-issue data to other third parties for their use. Plaintiffs also adequately alleged that Instacart's privacy policy only informs consumers that such information would only be disclosed to third parties in limited situations: to assist with the prevention or detection of fraud or for processing services. Plaintiffs have alleged sufficient facts to show that Stripe's disclosure to its merchants and customers was for purposes unrelated to fraud or the business services in this case.

The nature and volume of the collected information is also important. Plaintiffs allege that Stripe collected comprehensive information relating to plaintiffs' web browsing histories, financial information, device information, and online purchase activities. This information, according to plaintiffs, was then compiled into report, assigned a Risk Score, and then made available to all of Stripe's merchants for their personal use.

Taking plaintiffs' allegations, as required at this stage of litigation, the Court finds that plaintiffs' allegations that Stripe compiled and disseminated plaintiffs' sensitive data precludes the Court from finding that plaintiffs have no reasonable expectation of privacy. Thus, plaintiffs' allegations are sufficient to survive a motion to dismiss. Accordingly, the Court **DENIES** the motion as to plaintiffs' sixth and seventh causes of action.

F. UCL: Eighth Cause of Action

The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 865 (9th Cir. 2018) (citing Cal. Bus. & Prof. Code § 17200). Here, plaintiffs assert a UCL claim under all three prongs: unlawful, unfair, and fraudulent. The Court addresses each.

1. 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." *Cel-Tech Commc'ns., Inc. v. L.A. Cellular Telephone Co.*, 20 Cal.4th 163, 180 (1999) (quotation marks and citations 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." *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1225 (N.D. Cal. 2014) (quoting *Cel-Tech Commc'ns.*, 20 Cal.4th at 180).

Plaintiffs allege that Stripe's conduct is unlawful under the UCL because it violates: (i) CIPA §§ 631 and 635; (ii) the California Online Privacy Protection Act of 2003 ("CalOPPA"), Cal. Bus. & Prof. Code § 22575, *et seq.*; and (iii) and the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Bus. & Prof. Code § 1798, *et seq*. FAC ¶ 206.

With regards to the CIPA claims, the unlawful prong fails in light of the foregoing analysis.

With the remainder of the laws cited, the complaint does an inadequate job of explaining the specific violations of those statutes. This is especially so where, as Stripe correctly notes, the CCPA has no private right of action and on its face states that consumers may not use the CCPA as a basis for a private right of action under any statute. Cal. Civ. Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law."). Indeed, plaintiffs' opposition inappropriately attempts to explain the specific violations of CalOPPA where the complaint itself falls short. This is impermissible. *See e.g.*, *Harrison v. Robinson Rancheria Band of Pomo Indians Bus. Council*, No. 13-cv-01413-JST, 2013 WL 5442987, at *4 (N.D. Cal. Sept. 30, 2013) ("In their opposition brief, Plaintiffs offer a new theory . . . not hinted at in the complaint. 'It is axiomatic that the complaint may not be amended by briefs in opposition to a motion to dismiss.'").

Thus, plaintiffs' UCL claim under the unlawful prong fails. Accordingly, the Court **GRANTS** the motion to dismiss as to plaintiffs' cause of action on this ground.

2. Fraudulent

The "fraudulent" prong of the UCL "requires a showing [that] members of the public are likely to be deceived." *Wang v. Massey Chevrolet*, 97 Cal. App. 4th 856, 871 (2002). Claims stated under the fraud prong of the UCL are subject to the particularity requirements of Federal Rule of Civil Procedure 9(b). Under this Rule, in alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Plaintiffs must include an

account of the time, place, and specific content of the false representations at issue." *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016) (dismissing claims under the fraud prong of the UCL where plaintiffs failed to include an account of the time of the false representations at issue) (citations and quotations omitted).

Here, under this heightened standard, plaintiffs have not stated with sufficient particularity allegations to state a cause of action under the fraudulent prong of the UCL. Further, plaintiffs do not and cannot show that Stripe had an affirmative duty to disclose its data collection practices. "[A] failure to disclose a fact one has no affirmative duty to disclose is [not] 'likely to deceive' anyone within the meaning of the UCL." *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 838 (2006); *see also Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1557 (2007) ("Absent a duty to disclose, the failure to do so does not support a claim under the fraudulent prong of the UCL.").

Thus, plaintiffs' UCL claim under the fraudulent prong also fails. Accordingly, the Court **GRANTS** the motion as to plaintiffs' cause of action on this ground.

3. Unfair

There are two standards for determining what is "unfair competition" under the UCL. The first standard, in the context of claims brought by consumers, requires allegations that the challenged conduct violates a "public policy" that is "tethered" to a specific constitutional, statutory, or regulatory provision. *Gregory v. Albertson's, Inc.*, 104 Cal. App. 4th 845, 853 (2002). The second standard "involves balancing the harm to the consumer against the utility of the defendant's practice." *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 735 (9th Cir. 2007.)

Here plaintiffs argue that Stripe's conduct is unfair under the UCL because Stripe intruded on communications that plaintiffs reasonably believed to be private and then sold those communications to any of its customers and merchants that were ever involved in a transaction with plaintiffs. Plaintiffs also argue that the nature of Stripe's conduct offends public policy. To the extent plaintiffs' claims relate to Stripe's disclosure of plaintiffs' information, and not Stripe's collection of such information, the Court finds that the complaint sufficiently alleges facts to state

a claim under the unfair prong of the UCL. Plaintiffs' claims fail, however, to the extent that they rely on Stripe's collection of the information.

Accordingly, the Court **DENIES** the motion as to plaintiffs' cause of action under the unfair prong of the UCL.

G. Unjust Enrichment: Ninth Cause of Action

"To state a claim for unjust enrichment, Plaintiff must allege 'receipt of a benefit and unjust retention of the benefit at the expense of another.'" *Lectrodryer v. SeoulBank*, 77 Cal. App. 4th 723, 726 (Cal. Ct. App. 2000). In California, "there is not a standalone cause of action for 'unjust enrichment,' which is synonymous with 'restitution.'" *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015); *see also Brodsky v. Apple Inc.*, No. 19-cv-00712, 2019 WL 4141936, at *10 (N.D. Cal. Aug. 30, 2019) ("[C]ourts have consistently dismissed stand-alone claims for unjust enrichment."). Instead, at best, it is a species of fraud. *See Moose Run, LLC v. Libric*, No. 19-cv-01879-MMC, 2020 WL 3316097, at *5 (N.D. Cal. June 18, 2020) ("A cause of action titled 'unjust enrichment,' however, can be construed as a claim that the plaintiff is entitled to restitution under the theory 'the defendant obtained a benefit from the plaintiff by fraud.'"). To proceed on a theory based on fraud, the plaintiff "choose[s] not to sue in tort, but instead to seek restitution on a quasi-contract theory (an election referred to at common law as waiving the tort and suing in assumpsit)." *Id.*

Here, however, plaintiffs did not "waiv[e] the tort," but, rather, chose to "sue in tort," by also proceeding with their tort and statutory claims. Under such circumstances, plaintiffs are not entitled to restitution under a quasi-contract theory. *See id; In re Apple and AT&T iPad Unlimited Data Plan Litig.*, 802 F. Supp. 2d 1070, 1077 (N.D. Cal. 2011) ("plaintiffs cannot assert unjust enrichment claims that are merely duplicative of statutory or tort claims") (citing cases). This is especially so where plaintiffs have not alleged that they were "misled or that defendant breached any express or implied covenant as it relates" to the alleged conduct. *Doe v. Epic Games, Inc.*, 435 F. Supp. 3d 1024, 1052 (N.D. Cal. 2020). Moreover, this claim also fails in light of the Court's prior analysis as to fraud under the UCL.

Accordingly, the Court **Grants** the motion to dismiss as to plaintiffs' unjust enrichment

claims.

III. CONCLUSION

Based on the foregoing, the Court Orders:

- the motion to dismiss as to plaintiffs' first, second, third, and fourth causes of action is **GRANTED WITHOUT LEAVE TO AMEND**;
- the motion to dismiss as to plaintiffs' fifth cause of action is **DENIED** as to Ms. Alaina Jones, and **GRANTED WITHOUT LEAVE TO AMEND** as to the Utah Class;
- the motion to dismiss as to plaintiffs' sixth and seventh causes of action is **DENIED**;
- the motion to dismiss as to plaintiffs' eighth cause of action is **DENIED** as to the UCL's unfair prong but **GRANTED WITHOUT LEAVE TO AMEND** as to the fraud and unlawful prongs; and
- the motion to dismiss as to plaintiff's ninth cause of action is **GRANTED WITHOUT LEAVE TO AMEND**.

Stripe shall file an answer to plaintiffs' amended complaint within twenty-one (21) days from the date of this Order. The parties shall appear for a Case Management Conference on **MONDAY, AUGUST 30, 2021 AT 2:00 PM**.

This Order terminates Docket Number 48.

IT IS SO ORDERED.

Dated: July 28, 2021

YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT JUDGE

United States District Court
Northern District of California