UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JAMES COTTLE, et al.,
Plaintiffs,
v.
PLAID INC.,
Defendant.

Case No. 20-cv-03056-DMR

ORDER ON DEFENDANT'S MOTION TO DISMISS THE CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Re: Dkt. No. 78

This action consists of five separately-filed putative class actions in which 11 named plaintiffs allege that Defendant Plaid Inc. ("Plaid") uses consumers' banking login credentials to harvest and sell detailed financial data without their consent. The court consolidated the matters in July 2020 and Plaintiffs filed a consolidated amended class action complaint. [Docket No. 61 ("CFAC").] Plaid now moves pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) to dismiss the CFAC. [Docket No. 78.] The court held a hearing on February 11, 2021. For the following reasons, the motion is granted in part and denied in part.

I. FACTUAL BACKGROUND

Plaintiffs make the following allegations in the CFAC: Plaid is a tech startup in the financial technology or "fintech" industry. It provides bank "linking" and verification services for fintech apps that consumers use to send and receive money from their financial accounts, such as Venmo, Coinbase, Cash App, and Stripe (the "fintech apps"). CFAC ¶¶ 2, 32. Fintech apps typically verify accounts either by making micro-deposits to a user's account and then requiring the user to report the amounts back to the app, or by asking a user to log in to an account directly to confirm their status as account holder. *Id*. at ¶ 32.

According to Plaintiffs, consumers typically log into their banks from fintech apps via an "OAuth" procedure. Under this procedure, the app redirects users to their bank where they log in to their account, and then redirects users back to the fintech app. The bank returns a "token" that allows the fintech app to access the necessary bank information without giving the app access to the login information. *Id*. at ¶ 33.

Plaid does not use a true OAuth procedure. For the first several years of Plaid's operations, fintech apps collected user bank login information and passed that information to Plaid, which approached banks directly. Starting around 2016, Plaid implemented a new "Managed OAuth" system. Plaid designed the login screens in its interface to give them the look and feel of login screens used by individual financial institutions. According to Plaintiffs, Plaid fails to disclose to its users that they are not actually interfacing with their bank. This lulls users into a false sense of security resulting in "increased customer conversion." *Id*. at ¶¶ 34-37.

For example, when Venmo users are prompted to verify ownership of a bank account, they select their financial institution from a list. Users are then directed to a login screen branded with their bank's logo and color scheme, which gives users the impression that they have been directed away from Venmo to interact with their own financial institution. "In reality, they have been directed to a connection screen designed and inserted by Plaid within the Venmo app, and their communications are to Plaid instead of to their . . . financial institution." *Id*. at ¶ 38. On these bank-branded Plaid login screens, consumers enter their login information which is transmitted directly to Plaid, and Plaid uses the information to access their bank accounts. *Id*. at ¶ 39. Plaintiffs allege that Plaid's use of bank logos and color schemes and its overall interface design "are intentionally deceptive." *Id*. at ¶ 40. They further allege that Plaid designed its system to fool consumers into handing their login information to a third party. *Id*. "[A]t no time are users of [the fintech apps] informed that Plaid will receive and retain access to their financial institution account login credentials." *Id*. at ¶ 66.

Plaintiffs allege that this "scheme defies industry norms and consumers' reasonable expectations" and that consumers are "left in the dark" about Plaid's collection of banking account credentials. *Id*. at ¶¶ 42, 43. They further allege that Plaid fails to properly protect the sensitive information it acquires, and that it uses only a single level of encryption that "leaves login credentials open to interception" by malicious actors with minimal expertise. *Id*. at ¶ 47.

Additionally, Plaintiffs allege that by using the accumulated consumer bank login information, "Plaid has collected—and now stores, analyzes, and offers to its fintech clients for sale—a staggering amount of consumer banking data." *Id.* at ¶ 48. Once Plaid obtains the login information, it uses the credentials to obtain the maximum amount of data accessible to the consumer from the bank under the "pretense" that it has permission to do so. *Id.* at ¶ 49. This includes detailed banking information for an average of 3,700 transactions per consumer, as well as an average of 1,750 unique geolocations to which the transactions are mapped. *Id.* at ¶ 50. Plaid automatically updates its cache of private financial information every few hours. It also obtains any information available in the accounts to which it has access, including transactions, addresses, and contacts, as well as information about joint account holders, authorized users, and minor children's related accounts. *Id.* at ¶¶ 55-56.

Plaintiffs allege that Plaid routinely sells the consumer banking data it collects, including to the fintech apps who use its services. However, it fails to exercise control or oversight into how companies store and use the sensitive information they purchase from Plaid. *Id.* at ¶¶ 59-60. In addition, Plaid has obtained a "serious competitive advantage" by means of the data it has accumulated from consumers, "where developers are forced to rely upon Plaid's technology even to understand their own users' behavior." *Id.* at ¶ 65.

Plaintiffs allege that Plaid and the fintech apps conceal Plaid's conduct from users, because at no time are users ever informed that Plaid receives and retains access to their financial institution account login credentials. According to Plaintiffs, neither Plaid nor the apps inform users that Plaid uses their credentials to collect information "on the scale and for the duration that actually occurs," let alone that Plaid will make the information available for purchase. *Id.* at ¶ 66.

The CFAC contains an illustrative example of the Plaid software in the Venmo app from early 2020. The largest text on the screen states, "Venmo uses Plaid to link your bank." Underneath, smaller text states, "Secure: Transfer of your information is encrypted end-to-end" and "Private: Your credentials will never be made accessible to Venmo." *Id.* at ¶¶ 67-68. At the bottom of the screen is a large "Continue" button. Just above the Continue button, text in the smallest font on the screen states, "By selecting 'Continue' you agree to the Plaid End User

Privacy Policy." According to Plaintiffs, there is no visual indication that this last statement is a clickable hyperlink, and it is deemphasized so that a reasonable user would not clearly recognize it as a hyperlink. Nothing on this or on any subsequent screen requires the user to read through the linked policy, indicate that the user has read the terms, or indicate acceptance of the terms. Nothing on this screen or on any other fintech app that uses Plaid indicates what Plaid is or what it does. *Id.* at ¶ 70.[1]

Plaintiff alleges that in the unlikely event that a user actually clicked on the hyperlink, they would be redirected to Plaid's lengthy privacy policy, which is inadequate and misleading and keeps consumers "in the dark" about Plaid's role and conduct. *Id.* at ¶ 71, 76. For example, the privacy policy contains a statement about the various categories of information Plaid collects from a user's financial accounts, such as "[i]nformation about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction[.]" *Id.* at ¶ 71. Plaintiffs allege that this statement "deceives consumers who use Venmo into believing that it only collects information about transactions conducted using the Venmo app," and "thereby conceals the fact that it collects years' worth of transaction information entirely unrelated to the consumer's use of Venmo." *Id.* at ¶ 74(j). They also allege that the privacy policy fails to disclose essential facts about Plaid's collection practices, including its collection of bank login information and use of such information to access all available private information from consumers' accounts. *Id.* at ¶ 74(h). Plaintiffs allege that Plaid uses "a 'fine-print click-through' disclosure process that is inadequate to establish knowledge or consent to Plaid's practices by consumers, even if the policy itself had fully and sufficiently disclosed Plaid's true conduct (which it did not)." *Id.* at ¶ 74(g). They further allege that Plaid's privacy policy does not comply with the Gramm-Leach-Bliley Act ("GLBA") and California law. *Id.* at ¶¶ 87-88, 95-98.

[1] Plaintiffs allege that after this action was filed, Plaid redesigned certain aspects of its software incorporated in Venmo. The text linking users to Plaid's privacy policy is now in quotes and is underlined, and acts as a button that opens a new screen displaying certain information about the policy. Plaintiffs allege that none of the changes "have cured the deceptive nature of" Plaid's software. CFAC ¶¶ 72-73.

The Named Plaintiffs are:

- Carrie Anderson, a citizen and resident of New Hampshire. She alleges that she signed up to use the Venmo app in 2019 and the Cash App app in February 2020 via her mobile phone and that her TD Bank financial account was linked to and verified for use with the apps. She also alleges that her minor child's bank account is associated with her account and accessible via her own TD Bank username and password. CFAC ¶¶ 14, 100, 109, 110.
- James Cottle, a citizen and resident of California. He alleges that he signed up to use the Venmo app in January 2019 via his mobile phone and that his Wells Fargo Bank financial account was linked to and verified for use with the app. He also alleges that his minor child's bank account is associated with his account and accessible with his own Wells Fargo Bank username and password. *Id.* at ¶¶ 15, 111, 119, 120.
- Rachel Curtis, a citizen and resident of Florida. She alleges that she signed up to use the Venmo app in April 2015 via her mobile phone and that her USAA Bank financial account was linked to and verified for use with the app. *Id.* at ¶¶ 16, 121, 129.
- David Evans, a citizen and resident of California. He alleges that he signed up to use the Venmo app in mid-2016 via his mobile phone and that his UMe Federal Credit Union financial account was linked to and verified for use with the app. *Id.* at ¶¶ 17, 130, 139.
- Logan Mitchell, a citizen and resident of California. She alleges that she signed up to use the Venmo app in August 2015 and the Cash App app in September 2015 via her mobile phone and that her Chase Bank and California Coast Credit Union financial accounts were linked to and verified for use with the apps. *Id.* at ¶¶ 18, 140, 149.
- Alexis Mullen, a citizen and resident of Pennsylvania. She alleges that she signed up to use the Venmo app in March 2014 via her personal computer and that her TD Bank and PNC Bank financial accounts were linked to and verified for use with the app. *Id.* at ¶¶ 19, 150, 158.
- Jordan Sacks, a citizen and resident of the District of Columbia. He alleges that he

signed up to use the Venmo app in June 2014 via his personal computer and that his Chase Bank financial account was linked to and verified for use with the app. *Id*. at ¶¶ 20, 159, 167.

- Frederick Schoeneman, a citizen and resident of California. He alleges that he signed up to use the Venmo app in July 2016 via his mobile phone and that his Wells Fargo Bank financial account was linked to and verified for use with the app. *Id*. at ¶¶ 21, 168, 177.
- Gabriel Sotelo, a citizen and resident of California. He alleges that he signed up to use the Venmo app in early 2020 via his mobile phone and that his Bank of America financial account was linked to and verified for use with the app. *Id*. at ¶¶ 22, 178, 187.
- Jeffrey Umali, a citizen and resident of California. He alleges that he signed up to use the Venmo app in 2015, the Cash App app in 2016, and the Coinbase app in 2017 via his mobile phone. He further alleges that his Chase Bank financial account was linked to and verified for use with all three apps. *Id*. at ¶¶ 23, 188, 189, 198.
- Nicholas Yeomelakis, a citizen and resident of Massachusetts. He alleges that he signed up to use the Venmo app in March 2014 via his mobile phone and that his Bank of America financial account was linked to and verified for use with the app. *Id*. at ¶¶ 24, 199, 207.

Plaintiffs each allege that they do not recall being prompted to read any privacy policy from Plaid or having read any privacy policy from Plaid when they linked their financial accounts. They further allege that to the extent that they recall specific details of logging into their financial accounts in the Venmo, Cash App, and Coinbase apps, the details of logging in "are consistent with the discussion of Plaid's interface" in the CFAC. *Id*. at ¶¶ 101, 112, 122, 131, 141, 151, 160, 169, 179, 190, 200.

Based on the foregoing, Plaintiffs bring the following claims against Plaid: 1) invasion of privacy—intrusion into private affairs; 2) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; 3) violation of the Stored Communications Act, 18 U.S.C. § 2701 et seq.; 4) declaratory judgment and injunctive relief; 5) unjust enrichment (quasi-contract claim for restitution and disgorgement); 6) violation of California's Unfair Competition Law ("UCL"), California Business & Professions Code section 17200 et seq.; 7) violation of Article I, Section I of the California Constitution; 8) violation of the California Anti-Phishing Act of 2005, California Business & Professions Code section 22948 et seq.; 9) violation of California Civil Code sections 1709 and 1710; and 10) violation of California's Comprehensive Computer Data Access and Fraud Act, California Penal Code section 502.

Plaintiffs bring the first six claims on behalf of themselves and the following "Nationwide Class":

> All natural persons in the United States whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers, including without limitation users of Venmo, Square's Cash App, Coinbase, and Strike, from January 1, 2013 to the present.

Id. at ¶ 247. In addition, Cottle, Evans, Mitchell, Schoeneman, Sotelo, and Umali bring the seventh through tenth claims on behalf of themselves and the following "California class":

> All natural persons in California whose accounts at a financial institution were accessed by Plaid using login credentials obtained through Plaid's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers, including without limitation users of Venmo, Square's Cash App, Coinbase, and Strike, from January 1, 2013 to the present.

Id. at ¶ 248.

II. PROCEDURAL HISTORY

Plaintiffs filed their original complaints in five separate lawsuits in May, June, and July 2020. The court related the cases and subsequently consolidated them in one action, No. 20-cv-3056, *In re Plaid Inc. Privacy Litigation*, and granted the parties' request to appoint Interim Co-Lead Counsel and a Steering Committee. [Docket No. 57.] Pursuant to court order, Plaintiffs filed the CFAC on August 5, 2020. [Docket No. 61.] Plaid now moves to dismiss the CFAC. [Docket No. 78.]

III. LEGAL STANDARDS

Plaid moves to dismiss the CFAC pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

A. **Rule 12(b)(1)**

The question of standing is "an essential and unchanging part of the case-or-controversy requirement of Article III [of the U.S. Constitution]." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Because standing is a jurisdictional issue, it is properly addressed under a Rule 12(b)(1) motion. *Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1174 (9th Cir. 2004). A court will dismiss a party's claim for lack of subject matter jurisdiction "only when the claim is so insubstantial, implausible, foreclosed by prior decisions of th[e Supreme] Court, or otherwise completely devoid of merit as not to involve a federal controversy." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998) (citation and quotation marks omitted); *see* Fed. R. Civ. P. 12(b)(1). To satisfy Article III's standing requirements, a plaintiff must show "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).

"Where standing is raised in connection with a motion to dismiss, the court is to accept as true all material allegations of the complaint, and . . . construe the complaint in favor of the complaining party." *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 597 (9th Cir. 2020) (quotations omitted).

B. **Rule 12(b)(6)**

A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the claims alleged in the complaint. *See Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). When reviewing a motion to dismiss for failure to state a claim, the court must "accept as true all of the factual allegations contained in the complaint," *Erickson*, 551 U.S. at 94 (2007) (citation omitted), and may dismiss a claim "only where there is no cognizable legal theory" or there is an absence of "sufficient factual matter to state a facially plausible claim to relief." *Shroyer v. New*

Cingular Wireless Servs., Inc., 622 F.3d 1035, 1041 (9th Cir. 2010) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 677-78 (2009); *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001)) (quotation marks omitted). A claim has facial plausibility when a plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citation omitted). In other words, the facts alleged must demonstrate "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)); *see Lee v. City of L.A.*, 250 F.3d 668, 679 (9th Cir. 2001), overruled on other grounds by *Galbraith v. Cty. of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002).

As a general rule, a court may not consider "any material beyond the pleadings" when ruling on a Rule 12(b)(6) motion. *Lee*, 250 F.3d at 688 (citation and quotation marks omitted). However, "a court may take judicial notice of 'matters of public record,'" *id*. at 689 (citing *Mack v. S. Bay Beer Distrib*., 798 F.2d 1279, 1282 (9th Cir. 1986)), and may also consider "documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleading," without converting a motion to dismiss under Rule 12(b)(6) into a motion for summary judgment. *Branch v. Tunnell*, 14 F.3d 449, 454 (9th Cir. 1994), *overruled on other grounds by Galbraith*, 307 F.3d at 1125-26. The court need not accept as true allegations that contradict facts which may be judicially noticed. *See Mullis v. U.S. Bankr. Court*, 828 F.2d 1385, 1388 (9th Cir. 1987).

IV. REQUESTS FOR JUDICIAL NOTICE AND INCORPORATION BY REFERENCE

Plaid asks the court to take judicial notice of four documents and a series of screenshots from the Venmo app, and to consider the same materials under the incorporation by reference doctrine. [Docket No. 81 (Def.'s Request for Judicial Notice, "RJN").] Plaintiffs oppose the request. [Docket No. 109.] After the briefing on the motion to dismiss was complete, Plaintiffs moved for leave to file a supplemental RJN (Docket No. 115), to which Plaid did not file an opposition or response.[2]

[2] The parties requested and were granted leave to file oversized briefs in connection with the motion to dismiss. [Docket No. 75.] However, Plaid's request for judicial notice consisted of a

1. Legal Standard

A district court generally may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion. *Branch*, 14 F.3d at 453. If "matters outside the pleading are presented to and not excluded by the court," the court must treat the motion as a Rule 56 motion for summary judgment. *See* Fed. R. Civ. P. 12(d). "A court may, however, consider certain materials—documents attached to the complaint, documents incorporated by reference in the complaint, or matters of judicial notice—without converting the motion to dismiss into a motion for summary judgment." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). "Both of these procedures permit district courts to consider materials outside a complaint, but each does so for different reasons and in different ways." *Khoja v. Orexigen Therapeutics, Inc*., 899 F.3d 988, 998 (9th Cir. 2018). The Ninth Circuit recently cautioned courts about the appropriate use of judicial notice and the incorporation by reference doctrine when ruling on Rule 12(b)(6) motions:

> The overuse and improper application of judicial notice and the incorporation-by-reference doctrine . . . can lead to unintended and harmful results. Defendants face an alluring temptation to pile on numerous documents to their motions to dismiss to undermine the complaint, and hopefully dismiss the case at an early stage. Yet the unscrupulous use of extrinsic documents to resolve competing theories against the complaint risks premature dismissals of plausible claims that may turn out to be valid after discovery. . . . If defendants are permitted to present their own version of the facts at the pleading stage—and district courts accept those facts as uncontroverted and true—it becomes near impossible for even the most aggrieved plaintiff to demonstrate a sufficiently "plausible" claim for relief. Such undermining of the usual pleading burdens is not the purpose of judicial notice or the incorporation-by-reference doctrine.

Id. (internal citations omitted).

Federal Rule of Evidence 201 governs judicial notice. Under Rule 201, a court may take judicial notice of "an adjudicative fact if it is 'not subject to reasonable dispute.'" *Id.* at 999 (quoting Fed. R. Evid. 201(b)). A fact is "not subject to reasonable dispute" if it is "generally

five-page brief that it filed in addition to its 38-page motion to dismiss. For their part, Plaintiffs filed a seven-page opposition to the request for judicial notice, in addition to their 45-page opposition to the motion to dismiss. These submissions resulted in the parties' submissions going well beyond the already-enlarged page limits. Additionally, Plaid filed a separate four-page reply to Plaintiff's opposition to the RJN (Docket No. 112) as well as a supplemental RJN in support of its reply. [Docket No. 113.] As Plaintiffs were not given the opportunity to respond to the supplemental RJN, the court declines to consider it. In future motions, the parties should include any argument supporting or opposing requests for judicial notice within the main briefs.

known," or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). While a court may take judicial notice of matters of public record without converting a motion to dismiss into a motion for summary judgment, it may not take judicial notice of disputed facts stated in public records. *Lee*, 250 F.3d at 690. "Just because [a] document itself is susceptible to judicial notice does not mean that every assertion of fact within that document is judicially noticeable for its truth." *Khoja*, 899 F.3d at 999. If a court takes judicial notice of a document, it must identify the specific fact or facts it is noticing from the document. *Id.*

In contrast, the incorporation by reference doctrine is "a judicially-created doctrine that treats certain documents as though they are part of the complaint itself." *Id.* at 1002. This is to prevent "plaintiffs from selecting only portions of documents that support their claims, while omitting portions that weaken—or doom—their claims." *Id.* Incorporation by reference is appropriate "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *Id.* at 1002 (quoting *Ritchie*, 342 F.3d at 907). However, if a document "merely creates a defense to the well-pled allegations in the complaint, then that document did not necessarily form the basis of the complaint." *Id.* Further, "the mere mention of the existence of a document is insufficient to incorporate the contents of a document." *Id.* (quoting *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010)). The Ninth Circuit has instructed that "the doctrine is not a tool for defendants to short-circuit the resolution of a well-pleaded claim." *Id.* Thus, "while a court "may assume [an incorporated document's] contents are true for purposes of a motion to dismiss under Rule 12(b)(6) . . . it is improper to assume the truth of an incorporated document if such assumptions only serve to dispute facts stated in a well-pleaded complaint." *Id.*; *see also id.* at 1014 ("The incorporation-by-reference doctrine does not override the fundamental rule that courts must interpret the allegations and factual disputes in favor of the plaintiff at the pleading stage.").

2. Plaid's RJN

Exhibit A to Plaid's RJN is a copy of Plaid's End User Privacy Policy, effective December 30, 2019. Exhibit B is a copy of Venmo's Privacy Policy, effective June 30, 2020. Exhibit C is a copy of Cash App's Additional Cash Terms of Service—Annotated, effective April 16, 2019, and Exhibit D is a copy of Coinbase's Global Privacy Policy, effective July 31, 2020. [Docket No. 79 (Dettmer Decl., Sept. 14, 2020) ¶¶ 2-5, Exs. A-D.] Exhibit E is "a series of screenshots captured from the Venmo application under [attorney Ethan D. Dettmer's] supervision on August 31, 2020" that he asserts "show the consumer experience when connecting a bank account to Venmo using Plaid Link." Dettmer Decl. ¶ 6.

Plaid argues that the documents are judicially noticeable under Federal Rule of Evidence 201(b)(2) because they are "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." RJN 1. According to Plaid, Exhibits A through E are "publicly available" documents and images that are "not subject to reasonable dispute." *Id*. at 4-5.

Plaintiffs dispute the relevance of the materials. They note that the CFAC alleges that each Plaintiff signed up for the fintech apps at issue before the effective dates of the privacy policies and/or terms of service in those exhibits.[3] Therefore, according to the allegations in the CFAC, Plaid first accessed Plaintiffs' information before the effective dates of these policies. *See* CFAC ¶¶ 100, 111, 121, 130, 140, 150, 159, 168, 178, 188, 199. Similarly, Exhibit E consists of screenshots that purportedly document a registration process on August 31, 2020, well after Plaid allegedly accessed Plaintiffs' information. Accordingly, Plaintiffs contend that the documents and screenshots are not relevant to this motion. They also argue that Plaid seeks to use judicial notice to establish purported "facts" that are in dispute; whether any version of Plaid's privacy policy was disclosed to Plaintiffs and whether such disclosure would inform a reasonable consumer of Plaid's alleged conduct are factual questions that are subject to debate.

Given disputes about the meaning and relevance of these materials, the court declines to take judicial notice of Exhibits A through E. *See Khoja*, 899 F.3d at 1000 ("[i]t is improper to judicially notice a [document] when the substance of the [document] is subject to varying

[3] The court notes that there is one exception: the CFAC alleges that Anderson signed up to use the Cash App app in February 2020, which was after the April 16, 2019 effective date of the Cash App terms of service. CFAC ¶ 100. This does not change the outcome of Plaid's RJN.

interpretations, and there is a reasonable dispute as to what the [document] establishes." (internal quotation marks and citation omitted)).

Plaid also contends that the court should consider Exhibits A through E under the incorporation by reference doctrine. As to Exhibit A, Plaid's privacy policy, Plaid argues that Plaintiffs' claims "depend on the contents of the privacy policy." RJN 3. With respect to Exhibits B, C, and D, Plaid asserts that although Plaintiffs claim to have used Venmo, Cash App, and Coinbase, they "conspicuously omit their knowledge of [the apps']" policies and disclosures that "undermine their complaint." *Id.* at 3-4. Finally, as to the screenshots in Exhibit E, Plaid contends that Plaintiffs include a "subset" of these screenshots of the consumer experience when linking a bank account to Venmo using Plaid's software, and argues that "[t]he complete set of screenshots" refutes Plaintiffs' allegations that they would not have connected their bank accounts to Venmo had they known of Plaid's role. *Id.* at 5.

The court denies Plaid's request to consider Exhibits A through E under the incorporation by reference doctrine. Incorporation by reference is appropriate "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *Khoja*, 899 F.3d at 1002 (quotation omitted). The CFAC does not refer extensively to Plaid's privacy policies, and those policies are not the primary driver behind Plaintiffs' claims. Rather, Plaintiffs' statutory and common law claims are based on Plaid's alleged practices of deceptively obtaining consumers' banking credentials and using those credentials to improperly harvest and sell their private information. Plaid's privacy policies "create[ ] a defense" to these allegations, a defense that Plaintiffs expressly dispute in the CFAC. *See Khoja*, 899 F.3d at 1002 (if a document "merely creates a defense to the well-pled allegations in the complaint, then that document did not necessarily form the basis of the complaint."); CFAC ¶ 74 (alleging that the means by which Plaid discloses its privacy policy is "inadequate to establish knowledge or consent to Plaid's practices" and that Plaid's privacy policy does not "fully and sufficiently disclose[ ] Plaid's true conduct."). The sufficiency of Plaid's privacy policy is a key disputed issue in this case. Resolution of that issue is inappropriate at this stage. *See id.* at 1003 (noting that its admonition that "it is improper to assume the truth of an incorporated document if such assumptions only serve to dispute facts stated in a well-pleaded complaint" is "consistent with the prohibition against resolving factual disputes at the pleading stage.").

Finally, incorporation by reference is inappropriate because Plaintiffs dispute the relevance of these materials as well as their authenticity. Opp'n to RJN 6. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010) (incorporation by reference may be used where the complaint necessarily relies upon a document or the contents of the document are alleged in a complaint, the document's authenticity is not in question and there are no disputed issues as to the document's relevance."). As discussed above, the CFAF alleges violations that arose before the effective date of the materials contained in the exhibits.

3. Plaintiffs' RJN

On December 28, 2020, after the briefing on the motion to dismiss was complete, Plaintiffs moved for leave to file a supplemental RJN. They ask the court to take judicial notice of a complaint filed by The PNC Financial Services Group, Inc. ("PNC") against Plaid on December 21, 2020 in the United States District Court, Western District of Pennsylvania. Pls.' RJN Ex. A (*The PNC Financial Services Group, Inc. v. Plaid Inc.*, No. 2:20-cv-1977 (filed on Dec. 21, 2020), "PNC Complaint"). Plaid did not file an opposition or response.

The unopposed request is granted. Federal courts may "take notice of proceedings in other courts, both within and without the federal judicial system, if those proceedings have a direct relation to the matters at issue." *U.S. ex rel Robinson Rancheria Citizens Council v. Borneo, Inc.*, 971 F.2d 244, 248 (9th Cir. 1992). In its lawsuit, PNC alleges that Plaid "has sought to obtain trust and consumer confidence from consumers by intentionally designing user interfaces to misleadingly suggest that Plaid was affiliated or associated with, or sponsored by, PNC." It further alleges that Plaid did so "to mislead consumers into believing they are entering their sensitive personal and financial information in PNC's trusted and secure platform" or a platform associated with PNC in order to "persuade consumers to provide Plaid the consumer's sensitive financial information." PNC Compl. ¶¶ 4, 6.

The court concludes that judicial notice of the Western District of Pennsylvania proceeding is appropriate here. Plaintiff Mullen alleges that her accounts at PNC were linked to Venmo through Plaid, CFAC ¶ 158, and the CFAC alleges that banks, including PNC, have objected to Plaid's alleged practices and taken steps to prevent Plaid from accessing its banking customers' information for Venmo and other apps. *Id.* at ¶¶ 78-81. Additionally, Plaid argues that the allegation in the CFAC that it acted "without obtaining the approval or authority" of the financial institutions is unsupported and should be disregarded. Mot. 34 (citing CFAC ¶ 353). PNC's allegations are relevant to Plaintiff's response to that claim. Accordingly, the court takes judicial notice of the PNC Complaint.

V. DISCUSSION

Plaid moves to dismiss the CFAC on several grounds. It argues that 1) Plaintiffs lack standing under Article III; 2) most of Plaintiffs' claims are time-barred; 3) Plaintiffs' equitable claims fail because they have adequate legal remedies; and 4) Plaintiffs' claims fail as a matter of law. Additionally, Plaid argues that Plaintiffs' claims fail because they do not allege that they used Plaid to link their bank accounts to the fintech apps.[4] The court addresses this argument first before turning to the others.

A. Whether Plaintiffs Sufficiently Allege That They Linked Their Accounts Through Plaid

According to Plaid, Plaintiffs fail to allege that they actually linked their financial accounts to the fintech apps using Plaid. Instead, Plaintiffs allege only that they "signed up to use" certain apps that allow users to link their financial accounts through Plaid. *See, e.g.*, CFAC ¶ 100. Plaid argues that Plaintiffs therefore cannot proceed with their claims because they have "not implicated Plaid in the conduct they complain of." Mot. 7-8.

Plaid's argument is not persuasive. Plaintiffs allege that they are "App users who linked their financial accounts using Plaid's software integrated with the" fintech apps. CFAC ¶ 99. They also allege facts that describe how their bank accounts were linked to the apps in a manner

[4] Plaid also argues that its privacy policy clearly discloses its "data-processing practices," that the policy "makes clear that Plaid does 'not sell or rent personal information' that it collects," and that consumers connecting their financial accounts through Plaid "learn about Plaid's role and its Privacy Policy." Mot. 7. These arguments rely upon materials outside the CFAC that the court has declined to consider for purposes of adjudicating this motion. Accordingly, the court does not reach them.

consistent with Plaid's procedure. For example, Anderson alleges that when she signed up to use Venmo and Cash App, she logged into her bank account when prompted by the apps. *See, e.g.*, CFAC ¶¶ 102, 104. Each of the named Plaintiffs makes similar allegations. *Id*. at ¶¶ 113, 115, 123, 125, 132, 134, 142, 144, 152, 154, 161, 163, 170, 172, 180, 182, 191, 193, 201, 203. They also allege that to the extent that they recall specific details of logging into their accounts in the apps, the details of logging in "are consistent with the discussion of Plaid's interface" in the CFAC. *Id*. at ¶¶ 101, 112, 122, 131, 141, 151, 160, 169, 179, 190, 200. The CFAC also alleges the existence of an alternative to link a bank account without Plaid's involvement, describing a different process involving micro-deposits to a user's account where the user must report the amounts back to the app. *Id*. at ¶ 32. None of the Plaintiffs allege that they verified their accounts using this process. The court concludes that the allegations in the CFAC are sufficient to support the inference that Plaintiffs linked their financial accounts to the fintech apps using Plaid.

B. **Whether Plaintiffs Have Established Standing**

To satisfy Article III's standing requirements, a plaintiff must show "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth*, 528 U.S. at 180-81.

Plaid argues that Plaintiffs lack Article III standing to pursue their claims because they have failed to sufficiently plead an injury-in-fact, causation, and redressability.

1. Injury-in-Fact

Plaid argues that Plaintiffs allege only legally insufficient, hypothetical harms that are not concrete, actual, or imminent. Mot. 8-14. "To establish an injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized.'" *In re Facebook*, 956 F.3d at 597 (quoting *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016)). "For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" *Spokeo*, 136 S. Ct. at 1548. It must also be "concrete." *Id*. A concrete injury is one that "actually exist[s]"; that is, it must be "real, and not abstract," but it need not be tangible.

Id. at 1548-49 (quotation marks and citations omitted).

Plaintiffs argue that they have standing because each of their claims relates to Plaid's alleged invasion of their privacy rights. The court agrees. "A right to privacy 'encompass[es] the individual's control of information concerning his or her person." *In re Facebook*, 956 F.3d at 598 (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)). The Ninth Circuit has held that the disclosure of sensitive private information constitutes a "concrete and particularized" injury for purposes of Article III where plaintiffs "sufficiently allege[ ] a clear invasion of the historically recognized right to privacy." *In re Facebook*, 956 F.3d at 598-99. Such allegations are sufficient even in the absence of allegations of additional, tangible harm. *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784-85 (N.D. Cal. 2019) (collecting cases, holding that allegation that plaintiffs' "sensitive information was disseminated to third parties in violation of their privacy" was sufficient, by itself, to confer standing, even where no theft or hack of the information occurred and the "sensitive information" did not include social security or credit card numbers).

Here, Plaintiffs have sufficiently alleged an invasion of their privacy rights and corresponding harm. The CFAC alleges that Plaid embeds its software into fintech apps, and that when users seek to link their financial accounts to the apps, Plaid's software presents them with login screens that look like those used by their individual financial institutions. However, Plaid does not disclose to users that they are interfacing with Plaid rather than their banks. Once deceived, users provide their login information which is transmitted directly to Plaid, and Plaid uses the information to access their bank accounts. The CFAC further alleges that Plaid makes no effort to meaningfully disclose how it operates and deemphasizes the link to its privacy policy which Plaintiffs allege is itself substantively inadequate. Finally, Plaid uses the login information to obtain all available data about the users from their financial institutions, regardless of whether it relates to the fintech apps' money-transfer purposes. This includes information that shows users' "healthcare, educational, social, transportation, childcare, political, saving, budgeting, dining, entertainment, and other habits," along with corresponding geolocations. Plaid then sells this personal data to third parties. *See* CFAC ¶ 50. These allegations are sufficient to allege that

Plaid's data collection practices "would cause harm or a material risk of harm to [Plaintiffs'] interest in controlling their personal information." *See In re Facebook*, 956 F.3d at 599.

Plaid argues that Plaintiffs cannot establish standing under *In re Facebook* because Plaintiffs intended to provide their chosen fintech apps with access to their data which defeats their claim of unauthorized access. Plaid also asserts that Plaintiffs had the opportunity to control or prevent the purported "unauthorized" access of their private information by connecting without Plaid or disconnecting their accounts from the apps. Mot. 13. In other words, Plaid contends that Plaintiffs consented to, or were informed of and failed to try to stop Plaid's data collection practices. To begin with, this ignores the allegations in the CFAC that Plaintiffs were unaware of, and did not consent to, Plaid's practices. *See* CFAC ¶ 74(g). Moreover, this argument goes to the merits of Plaintiffs' claims, but the question of standing is "distinct from the merits." *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011); *see also In re Facebook, Inc., Consumer Privacy*, 402 F. Supp. 3d at 788 ("in virtually every privacy case, consent will be part of the merits inquiry. Because courts presume success on the merits when evaluating standing, these are not standing issues in privacy cases.").

Finally, Plaid argues that the express disclosures in its privacy policy defeat Plaintiffs' invasion of privacy allegations. Mot. 13. This argument rests on materials outside the CFAC that the court cannot consider. As discussed above, it also presents a merits issue that does not defeat standing.

2. Causal Connection Between Plaintiffs' Injury and Plaid's Conduct

Plaid argues that Plaintiffs have failed to allege that Plaid caused them injury. In order to establish "a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (internal quotation marks and citation omitted).

Plaid's sole argument is that the CFAC does not allege that Plaintiffs linked their accounts to the fintech apps using Plaid, and that as a result, they have not alleged that Plaid caused harm. Mot. 14. As discussed above, the allegations in the CFAC are sufficient on this point.

Accordingly, Plaintiffs have sufficiently alleged a causal connection between the claimed injury and Plaid's alleged conduct.

3. Redressability

Plaid asserts that Plaintiffs fail to plead how their injuries are "likely to be redressed by a favorable decision," and that any relief would provide only "psychic satisfaction," which is an unacceptable Article III remedy. Mot. 14-15 (quoting *Steel*, 523 U.S. at 107). The court disagrees. Unlike the plaintiff in *Steel*, which sought civil penalties that were payable to the United States Treasury as well as declaratory relief that the Supreme Court deemed "worthless," 523 U.S. at 106, Plaintiffs seek damages and injunctive relief, among other remedies. *See Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 912 (9th Cir. 2011) (holding that "[t]here [was] no real question about redressability" where the plaintiff sought the available remedies of an injunction and damages). Moreover, "the Ninth Circuit has repeatedly explained that intangible privacy injuries can be redressed in the federal courts." *In re Facebook, Inc., Consumer Privacy*, 402 F. Supp. 3d at 784. Therefore, Plaintiffs have satisfied the third prong of the Article III standing requirement.

In sum, Plaid's motion to dismiss the CFAC based on lack of Article III standing is denied.

C. Whether Plaintiffs' Claims are Time-Barred

Plaid next argues that the "vast majority" of Plaintiffs' claims are barred by the applicable statutes of limitation.[5] Plaid contends that Plaintiffs' claims accrued when they signed up to use the fintech apps; it provides a bullet-pointed list of time-barred claims based on a chart in counsel's supporting declaration. Mot. 15; Dettmer Decl. ¶ 7.

Defendant provides no analysis of the timeliness of Plaintiffs' claims. It merely cites a California Supreme Court opinion in a products liability case holding that "[g]enerally speaking, a cause of action accrues at 'the time when the cause of action is complete with all of its elements.'" *See* Mot. 15 (quoting *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806 (2005)). It is not the court's job to make Plaid's arguments for it. In the absence of a more fulsome argument, the

[5] For purposes of this motion, Plaid concedes that certain claims are not time-barred. Mot. 15 n.12.

court denies Plaid's motion to dismiss any of Plaintiffs' claims as untimely. *See also Fox*, 35 Cal. 4th at 810 (holding that "[r]esolution of the statute of limitations issue is normally a question of fact.").

D. Whether Plaintiffs May Bring Equitable Claims

Plaid argues that the equitable claims for declaratory judgment, injunctive relief, unjust enrichment and unfair competition are barred because Plaintiffs have an adequate remedy at law.[6] Plaintiffs do not oppose Plaid's motion to dismiss their declaratory judgment and injunctive relief claim on the basis that it is not a standalone claim for relief. Opp'n 19 n.19. The court dismisses that claim with prejudice. Therefore, only Plaintiffs' unjust enrichment and UCL claims are at issue with respect to this argument.

Plaid asserts that these claims should be dismissed because Plaintiffs seek damages that would compensate them for all harms they allegedly suffered and do not claim that such damages are inadequate. Mot. 17. In support, it cites a string of cases dismissing similar claims at the pleading stage where the plaintiffs alleged other claims that present an adequate legal remedy. *See id.* (citations omitted). However, other courts in this district have denied motions to dismiss equitable claims because plaintiffs may pursue alternative remedies at the pleading stage. *See, e.g., Adkins v. Comcast Corp.*, No. 16-CV-05969-VC, 2017 WL 3491973, at *3 (N.D. Cal. Aug. 1, 2017) (stating that the court "is aware of no basis in California or federal law for prohibiting the plaintiffs from pursuing their equitable claims in the alternative to legal remedies at the pleadings stage"); *Aberin v. Am. Honda Motor Co., Inc.*, No. 16-CV-04384-JST, 2018 WL 1473085, at *9 (N.D. Cal. Mar. 26, 2018) (finding that there is "no bar to the pursuit of alternative remedies at the pleadings stage"); *Marshall v. Danone US, Inc.*, 402 F. Supp. 3d 831, 834 (N.D. Cal. 2019) (stating "the *Adkins* and *Aberin* approach appears more consistent with ordinary pleading principles" and denying motion to dismiss claims seeking only equitable relief, including UCL claim). The court agrees with the reasoning of these cases and denies the motion to dismiss

[6] Plaid originally moved to dismiss Plaintiffs' equitable claims *and* remedies. Mot. 16-17. It clarifies in its reply that it "only seeks the dismissal of Plaintiffs' equitable claims, not all equitable remedies Plaintiffs may pursue through their legal claims." Reply 11 n.7. Plaid therefore withdraws its request that the court dismiss Plaintiffs' equitable remedies. *Id.*

Plaintiffs' unjust enrichment and UCL claims on the pleadings.

E. Whether Plaintiffs Have Adequately Alleged Their Claims

1. UCL

Plaintiffs' sixth claim is for violation of the UCL.[7] The UCL prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. "Because Business and Professions Code section 17200 is written in the disjunctive, it establishes three varieties of unfair competition—acts or practices which are unlawful, or unfair, or fraudulent." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). A UCL claim may only be brought by "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Therefore, to satisfy the UCL's standing requirements, a plaintiff must "demonstrate some form of economic injury," such as surrendering more or acquiring less in an transaction, having a present or future property interest diminished, being deprived of money or property, or entering into a transaction costing money or property that would otherwise have been unnecessary. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011).

Plaid argues that the UCL claim must be dismissed because Plaintiffs have not alleged that they lost money or property as a result of its alleged conduct. Plaintiffs' brief offers two theories: first, they argue that they suffered economic injury "in the form of lost indemnity rights that existed when Plaintiffs' data was held at their banks." Opp'n 23. This is based on the allegation that as a result of Plaid's conduct, Plaintiffs lost "valuable indemnity rights" that they possess under federal regulations which limit consumers' liability for unauthorized transfers. CFAC ¶¶ 215-216. According to the CFAC, banks have taken the position that "the provision of login credentials may be construed as a grant of 'authority' to conduct funds transfers" and thus they are not liable for unauthorized transfers. *Id.* at ¶¶ 217-219. Plaintiffs allege that in light of the banks' stance, Plaid's collection and use of consumers' bank login information "deprive[s] those consumers of rights to be indemnified and reimbursed for the amount of" unauthorized transfers.

[7] The court discusses the sufficiency of the claims in the order in which the parties addressed them in their briefs.

Id. at ¶ 221. Notably, the CFAC does not allege that any unauthorized transfers or fraudulent charges have taken place, let alone that banks have refused to indemnify users. This theory of economic damage is insufficient to establish a UCL claim because it is "hypothetical and conjectural" and not "concrete and particularized" and "actual or imminent." *See Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1049 (9th Cir. 2017) (holding that theory of economic injury for UCL based on eventual future price increases for unlimited text messaging service was "hypothetical and conjectural").

Plaintiffs' second theory fares no better. They highlight the allegations that "they would not have connected their bank accounts to the Apps the way they did . . . if they had known the truth about Plaid's role and its practices." Opp'n 23. Although Plaintiffs do not explain this argument in any detail, it appears to be based on the statement in *Kwikset* that a plaintiff may show an economic injury where they were "required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *See* 51 Cal. 4th at 323. That theory does not work here because Plaintiffs do not allege that they paid any money to Plaid for its services. *See, e.g., In re Facebook, Inc., Consumer Privacy*, 402 F. Supp. 3d at 804 (noting "the plaintiffs here do not allege that they paid any premiums (or any money at all) to Facebook to potentially give rise to standing under California law" for purposes of UCL claim and dismissing claim for failure to allege "lost money or property"); *Wesch v. Yodlee,* Inc., No. 20-cv-05991-SK, 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021) (holding that the plaintiffs had not alleged that they "surrender[ed] more or acquir[ed] less in a transaction than they otherwise would have" for purposes of UCL standing where they had not paid money to the defendant).

At the hearing, Plaintiffs offered an additional theory of economic injury: the loss of the inherent value of their personal data. [Docket No. 123 (Feb. 11, 2021 Hr'g Tr.) at 19-20.] They cite *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 440 F. Supp. 3d 447, 461-62 (D. Md. 2020). *Marriott* is readily distinguishable. It held that the loss of property value in personal identifying information in connection with a data breach was sufficient to establish injury-in-fact for purposes of constitutional standing; it did not consider whether that loss constituted economic injury for purposes of the UCL. Moreover, the Ninth Circuit has rejected a similar theory in an unpublished decision. In *In re Facebook Privacy Litig*., 572 Fed. Appx. 494, 494 (9th Cir. 2014), the court held that the loss of sales value of personal information disclosed by a defendant was sufficient to "to show the element of damages" for breach of contract and fraud claims. At the same time, it affirmed the dismissal of the plaintiffs' UCL claim "because plaintiffs failed to allege that they 'lost money or property as a result of the unfair competition.'" *Id*. (citing Cal. Bus. & Prof. Code § 17204)); *see also Adkins v. Facebook, Inc.*, No. C 18-05982 WHA, 2019 WL 3767455, at *3 (N.D. Cal. Aug. 9, 2019) (noting that the Ninth Circuit rejected the theory that the "lost value of [the plaintiff's] personal information" establishes standing under the UCL in *In re Facebook Privacy Litigation* and denying leave to amend based on that theory).[8]

Plaintiffs offer no other theory of economic injury. The court concludes that Plaintiffs' UCL claim must be dismissed based on their failure to allege that they lost money or property as a result of Plaid's alleged conduct.[9]

2. Computer Fraud and Abuse Act and Comprehensive Computer Data Access and Fraud Act

Plaintiffs' second and tenth claims are for violation of the federal Computer Fraud and Abuse Act ("CFAA") and its California corollary, the Comprehensive Computer Data Access and Fraud Act ("CDAFA").

a. CFAA

"The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1069 (N.D. Cal. 2018) (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130-31 (9th Cir. 2009)). "[T]he

[8] Plaintiffs filed a statement of the recent decision in *Calhoun v. Google*, 20-cv-05146-LHK, 2021 WL 1056532, at *22 (N.D. Cal. Mar. 17, 2021) (finding that plaintiffs had adequately alleged economic injury for a UCL claim based on the loss of value of personal information). [Docket No. 124.] This court disagrees with the holding in *Calhoun*. It rests on four cases that address Article III standing, which is different from UCL standing.

[9] As Plaintiffs have not sufficiently alleged an economic injury for purposes of the UCL claim, the court need not reach Plaid's remaining UCL arguments.

CFAA is 'an anti-hacking statute,' not 'an expansive misappropriation statute.'" *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir. 2019). Plaintiffs allege violations of six subsections of the CFAA. CFAC ¶¶ 273-296.

Plaid moves to dismiss the CFAA claims on several grounds. One argument is that Plaintiffs have not alleged facts supporting the requisite "damage or loss." In order to bring a civil action under the CFAA, a person must "suffer[ ] damage or loss by reason of a violation" of the statute. 18 U.S.C. §§ 1030(g). Specifically, Plaintiffs must allege "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. §§ 1030(g); 1030(c)(4)(A)(i)(I).[10] "The term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Thus, while 'damage' covers harm to data and information, 'loss' refers to monetary harms sustained by the plaintiff." *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 961 (N.D. Cal. 2014). The Ninth Circuit has held that "[t]he statute's 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself." *Andrews*, 932 F.3d at 1263.

Plaintiffs argue that they have pleaded the requisite elements of these claims, "including losses of at least $5,000 during a one-year period," based on the "lost value of their indemnification rights." Opp'n 27-28; *see* CFAC ¶ 297 (alleging losses in the amount of $5,000 during a one-year period). According to Plaintiffs, this sum is an aggregation across class members to meet the $5,000 minimum. Plaintiffs do not offer any authority to support that a bare allegation of lost indemnification rights, without facts supporting that a financial institution has

[10] The CFAA provides other methods of establishing "damage or loss" to support a civil action, none of which apply here. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(II-V).

actually refused to indemnify any Plaintiff, is a "loss" within the meaning of the CFAA. *See* Opp'n 28. For the reasons discussed above in connection with Plaintiffs' UCL claim, the court finds that an allegation about the potential loss of indemnification rights is insufficient to plead the requisite loss under the CFAA because it is speculative.

At the hearing, Plaintiffs offered several additional theories of loss for purposes of the CFAA: "the loss of the . . . right to control [Plaintiffs'] own data"; the "loss of the value of that data" after Plaid allegedly sold it; and the loss of protection over the data after Plaid allegedly removed it from a secure environment, including the increased risk of identity theft resulting from removing the data from a secure environment. Hr'g Tr. 28-29, 34-35; *see* CFAC ¶¶ 225-235. As to the first, the CFAC alleges only that "Plaintiffs and Class members suffered loss of use and control to Plaid of their own sensitive financial information, property which has value to them." CFAC ¶ 228. Plaintiffs do not explain how to value the alleged "loss of use and control" of their financial information and offer no authority that such a loss is cognizable for purposes of the CFAA.

The second theory Plaintiffs offered at the hearing is that the loss under the CFAA is the value of Plaintiffs' financial information. The CFAC alleges that Plaintiffs' sensitive financial information has "significant present financial value" and "significant future financial value," given that "Plaid has built a very successful business . . . of selling that information" and that it "plans to pivot and focus on monetizing that information . . ." CFAC ¶¶ 229-230 (emphasis removed). According to Plaintiffs, they "suffered harm when Plaid took their property, sold it, and put it to use for present and future monetization in other forms, for its own enrichment." *Id.* at ¶ 231. The Ninth Circuit's decision in *Andrews* forecloses this theory. In *Andrews,* the plaintiff asserted loss under the CFAA as the denial of profits that might have been received "from commodifying the personal information that [the defendant] allegedly obtained through unlawful means." 932 F.3d at 1262. The plaintiff argued that because the defendant "allegedly 'stole the personal information without compensating [him], he lost the value of that information and the opportunity to sell it,'" and that his claim satisfied the CFAA's $5000 threshold by virtue of the number of individuals in the putative class from whom the defendant obtained "valuable personal information." *Id.* The

Ninth Circuit rejected Plaintiff's theory, stating that the CFAA's "narrow [statutory] conception of 'loss' . . . does not include a provision that aligns with [plaintiff's] theory." *Id.*; *see also id.* at 1263 (noting that "any theory of loss must conform to the limited parameters of the CFAA's definition.").

Finally, Plaintiffs contend that Plaid's actions have resulted in "diminished value of [Plaintiffs'] rights to protection of their banking data" after Plaid removed the information from the banks' "trusted, secure environment," as well as loss due to the corresponding increased risk of identity theft and fraud to Plaintiffs after Plaid removed their data from a secure environment. CFAC ¶¶ 225, 232. However, the CFAC does not allege that any Plaintiff has suffered an actual, concrete loss as a result of losing "protection of their banking data," or that any Plaintiff has experienced identity theft or fraud resulting from Plaid's removal of their financial data from a secure banking environment. It also does not allege that any Plaintiff has incurred loss associated with taking steps to prevent identity theft or fraud. The court concludes that these allegations are insufficient to plead loss under the CFAA because they are entirely speculative.

In sum, the court concludes that the CFAC fails to plead cognizable loss of at least $5,000 in value. Accordingly, the CFAA claims are dismissed.[11]

b. CDAFA

The CDAFA "prohibits certain computer-based conduct such as '[k]nowingly and without permission access[ing] or caus[ing] to be accessed any computer, computer system, or computer network.'" *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1217 (N.D. Cal. 2014) (quoting Cal. Penal Code § 502(c)(7)). Plaintiffs allege violations of seven subsections of the CDAFA. CFAC ¶¶ 369-375.[12]

[11] Given the court's conclusion that Plaintiffs have not satisfied the damage or loss elements of these claims, it does not reach Plaid's remaining arguments in favor of dismissal of these claims.

[12] The provisions at issue hold liable any person who:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

As with the CFAA claims, Plaid argues that Plaintiffs lack standing to bring claims under the CDAFA because they have not alleged the requisite "damage or loss." The CDAFA provides that only an individual who has "suffer[ed] damage or loss by reason of a violation" of the statute may bring a civil action "for compensatory damages and injunctive relief or other equitable relief." Cal. Penal Code § 502(e)(1). The CDAFA permits recovery of "[c]ompensatory damages [that] include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id.* Unlike the CFAA, the CDAFA does not define "damage" or "loss," and does not contain a specific monetary threshold for loss related to violations of the statute. *See Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780 JW, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010).

Plaintiffs argue that they have suffered "damage or loss" under CDAFA in the form of "the lost value of their indemnification rights." As with their CFAA claims, they offer no authority that the potential loss of the right to indemnification without more is sufficient to support a

---

> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services.
>
> (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
>
> . . .
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
>
> (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

Cal. Penal Code § 502(c).

CDAFA claim. *See* Opp'n 28. The CFAC does not plead facts supporting actual damage or loss to Plaintiffs as a result of Plaid's alleged CDAFA violations. *See, e.g.*, *Facebook, Inc.*, 2010 WL 3291750, at *4-5 (holding that facts that plaintiff "expended resources to stop [defendant] from committing acts" that allegedly constituted CDAFA violations were sufficient to demonstrate that plaintiff "has suffered some damage or loss" to establish standing to bring suit under Section 502(e)). Additionally, Plaintiffs offer no support for their theories that the loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data, as discussed above, is "damage or loss" within the meaning of the CDAFA. *See, e.g.*, *Nowak v. Xapo, Inc.*, No. 5:20-cv-03643-BLF, 2020 WL 6822888, at *4-5 (N.D. Cal. Nov. 20, 2020) (dismissing CDAFA claim based on loss of value of stolen cryptocurrency in part because the nature of the loss was not cognizable under CDAFA).

Given the CFAC's failure to plead that Plaintiffs have suffered "damage or loss" due to the alleged Section 502 violations, the court dismisses the CDAFA claims.[13]

3. Stored Communications Act

Plaintiffs' third claim is for violation of the Stored Communications Act, or "SCA." The SCA allows a plaintiff to bring an action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a). The Ninth Circuit has explained that "[l]ike the tort of trespass, the [SCA] protects individuals' privacy and proprietary interests. . . . Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, . . . the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) (internal citations omitted).

The CFAC alleges SCA claims for unlawful access under section 2701(a)(1) and for

[13] As Plaintiffs have not sufficiently pleaded "damage or loss by reason of a violation" of Section 502, it does not reach Plaid's other arguments in favor of dismissal of these claims.

exceeding authorization under section 2701(a)(2). CFAC ¶¶ 307-308. In order to state a claim under either provision, Plaintiffs must allege that Plaid "(1) gained unauthorized access to a 'facility' where it (2) accessed an electronic communication in 'electronic storage.'" *In re Facebook*, 956 F.3d at 608 (quoting 18 U.S.C. § 2701(a)). The term "electronic communication" means

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
>
> **(A)** any wire or oral communication;
>
> **(B)** any communication made through a tone-only paging device;
>
> **(C)** any communication from a tracking device (as defined in section 3117 of this title); or
>
> **(D)** electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds[.]

18 U.S.C. §§ 2711(1), 2510(12). The term "electronic storage" means

> **(A)** any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> **(B)** any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]

18 U.S.C. §§ 2711(1), 2510(17). The SCA does not define the term "facility." *See In re Facebook*, 956 F.3d at 608, 609 n.10 (declining to decide whether "personal computers, web browsers, and browser managed files are 'facilities,' through which electronic communications service providers operate").

Plaintiffs' SCA claims are pleaded as follows:

> Plaid violated 18 U.S.C. § 2701(a)(1) when it intentionally accessed Plaintiffs' and Class members' financial institutions and their systems and databases without authorization, and thereby obtained access to the contents of Plaintiffs' and Class members' electronic communications while those communications were in electronic storage on such systems. Plaid's access to the banks' computer systems was not authorized by Plaintiffs or the financial institutions.
>
> Plaid's access to these facilities was achieved through subterfuge.

> Insofar as Plaid obtained purported authorization for its conduct, Plaid exceeded any such authorization by collecting, aggregating, selling, and divulging the contents of Plaintiffs' and Class members' electronic banking communications that were unrelated to the purpose for which Plaintiffs used the Participating Apps. 18 U.S.C. § 2701(a)(2). Plaid acquired communications far in excess of any information necessary to the Participating Apps for which account verification and linking were undertaken.

CFAC ¶¶ 307, 308. Plaintiffs assert that the SCA "facilities" are each of the financial institutions that are linked with the fintech apps. Each financial institution "provides its users with the ability to send and receive electronic communications, including, inter alia, images, data, queries, messages, notifications, statements, forms, updates, and intelligence regarding the financial institutions . . . as well as about customers' individual accounts and activities." *Id.* at ¶ 302. Further, they allege that "Plaintiffs' and Class members' financial institution[s] store the communications alleged herein in their respective systems and databases and on their respective servers . . . for purposes of backup protection of such electronic communications." *Id.* at ¶¶ 303, 305.

Plaid argues that Plaintiffs cannot state claims under the SCA for three reasons: 1) their financial institutions are not "facilities" under the SCA; 2) Plaintiffs have not sufficiently alleged that Plaid accessed an "electronic communication" under section 2701(a); and 3) Plaintiffs have not plausibly alleged that Plaid accessed an electronic communication "while it [was] in electronic storage." Mot. 29-30.

First, Plaid argues that a financial institution is not "a facility through which an electronic communication service is provided" under section 2701(a), citing *Central Bank & Trust v. Smith*, 215 F. Supp. 3d 1226, 1235 (D. Wyo. 2016) (holding that a bank was "not a facility under the [SCA]" because it was not "an internet service provider or analogous to one"). As noted, neither the SCA nor the Ninth Circuit have defined the term "facility through which an electronic communication service is provided." In *In re Facebook*, the Ninth Circuit observed that "the text and legislative history of the SCA demonstrate that its 1986 enactment was driven by congressional desire to protect third-party entities that stored information on behalf of users." 956 F.3d at 609 (citing *Hately v. Watts*, 917 F.3d 770, 782 (4th Cir. 2019) (Congress enacted the SCA to "protect against potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails")). Since its enactment, "the SCA has typically only been found to apply in cases involving a centralized data-management entity; for instance, to protect servers that stored emails for significant periods of time between their being sent and their recipients' reading them." *In re Facebook*, 956 F.3d at 609; *see also Theofel*, 359 F.3d at 1072-73 (the SCA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility"); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (discussing legislative history and concluding that "Congress' intent was to protect communications held in interim storage by electronic communication service providers"). One court in this district has noted that "uncontroversial examples of facilities that provide electronic communications services" include "the computer systems of an email provider, a bulletin board system, or an ISP." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012) (holding that iOS devices such as iPhones are not "facilities" under the SCA).

Plaintiffs do not address *In re Facebook*'s discussion of the SCA or its legislative history. They cite an out-of-circuit case holding that Facebook's server is a facility under the SCA where the plaintiff alleged that "Facebook provides its users with the ability to send and receive electronic messages." Opp'n 36 (citing *Decoursey v. Sherwin-Williams Co.*, No. 19-02198-DDC-GEB, 2020 WL 1812266, at *6 (D. Kan. Apr. 9, 2020)). Building on *Decoursey*, Plaintiffs argue that their financial institutions are analogous to Facebook's server because the banks "communicate information about [Plaintiffs'] financial affairs . . ." Opp'n 36; CFAC ¶ 302. The fact that an entity communicates electronically with its customers does not mean that it "provides an electronic communication service," and Plaintiffs offer no authority to support their sweepingly broad position. *See Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270-72 (N.D. Cal. 2001) (holding that "Amazon's own computer system" does not provide an electronic communications service and is not a "facility" under the SCA). Plaintiffs' argument that their financial institutions meet the SCA definition of "facility through which an electronic communication service is provided" is unsupported as well as inconsistent with the purpose of the SCA. This is fatal to the SCA claim.

Additionally, the CFAC does not plausibly allege that Plaid accessed an electronic communication while it was "in electronic storage." Plaintiffs allege that the communications at issue were in electronic storage because they were stored "for purposes of backup protection of such electronic communications." CFAC ¶ 305; *see* 18 U.S.C. § 2510(17)(B). They assert that "[f]inancial institutions necessarily store historical communications regarding a customer's past banking activities, historical direct messages, and other communications so that they may be accessed by consumers[.]" CFAC ¶ 305. However, data is considered stored "for purposes of backup protection" only if there is some other version of the data that is being backed up, which the CFAC does not allege. *See Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1044-46 (N.D. Cal. 2018) (holding § 2510(17)(B) was inapplicable to emails "because there is no other version of the email that is being backed up") (citing *Theofel*, 359 F.3d at 1077 ("A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes" under § 2510(17)(B))); *see also Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1088 (N.D. Cal. 2018) (dismissing SCA claim for failure to plausibly allege that communications stored on servers was "backup information"). In the absence of allegations that Plaintiffs' financial institutions store their "electronic banking communications" for the purpose of providing backup protection, the CFAC does not allege that Plaid accessed an electronic communication while it was "in electronic storage."

While the "in electronic storage" defect could potentially be addressed through amendment, the allegations regarding an SCA "facility" cannot. Accordingly, the SCA claim is dismissed.[14]

4. Invasion of Privacy—Intrusion into Private Affairs and Article I, Section I of the California Constitution

The parties combined their discussion of Plaintiffs' first claim for invasion of privacy—intrusion into private affairs and seventh claim for violation of the California Constitution's right

[14] As the court finds that Plaintiffs have not adequately alleged that their financial institutions are "facilities" or that Plaid accessed their communications while they were in "electronic storage," it does not reach Plaid's remaining argument in favor of dismissal of this claim.

to privacy. Accordingly, the court analyzes them together.

To state a claim for intrusion, a plaintiff must allege (1) that the defendant "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy" and (2) that the intrusion "occur[red] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsdale*, 47 Cal. 4th 272, 286 (2009). To state a claim for invasion of privacy under the California Constitution, a plaintiff must allege (1) "possess[ion] of a legally protected privacy interest"; (2) a reasonable expectation of privacy; and (3) "that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." *Id*. at 287 (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 35, 36-37 (1994)). "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook*, 956 F.3d at 601.

Plaid again argues that Plaintiffs cannot plausibly allege a reasonable expectation of privacy because they chose to link their accounts to the fintech apps and Plaid's privacy policy discloses the information it collects. It notes that Plaintiffs have never taken action to stop "the alleged invasion" by disconnecting their accounts or asking Plaid to delete their data. Mot. 31. Plaid further argues that Plaintiffs' allegations do not show an "egregious breach of the social norms." *Id*. at 32.

Plaid's positions are not persuasive. As discussed above, the question of whether Plaintiffs consented to Plaid's collection of their personal information is a key factual dispute to be decided on the merits rather than a Rule 12 motion. Whether Plaid's alleged conduct "could highly offend a reasonable individual," is also "an issue that cannot be resolved at the pleading stage." *In re Facebook*, 956 F.3d at 606. Plaintiffs have adequately stated claims for intrusion and violation of the California Constitution's right to privacy. *See In re Facebook, Inc., Consumer Privacy*, 402 F. Supp. 3d at 797 (holding that "plaintiffs have adequately alleged that they suffered an egregious invasion of their privacy when Facebook gave app developers and business partners their sensitive information on a widespread basis.").

5. California's Anti-Phishing Act of 2005

Plaintiffs' eighth claim is for violation of California's Anti-Phishing Act of 2005. That statute makes it unlawful for "any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes "[b]ank account number," "[p]ersonal identification number (PIN)," "[a]ccount password," and "[a]ny other piece of information that can be used to access an individual's financial accounts or to obtain goods or services." Cal. Bus. & Prof. Code § 22948.1(b). "An individual who is adversely affected by a violation of Section 22948.2 may bring an action . . . against a person who has directly violated Section 22948.2." Cal. Bus. & Prof. Code § 22948.3(a)(2).

According to Plaid, Plaintiffs have not stated a plausible section 22948.2 claim because "[t]his law does not apply to Plaid—which provides valuable services to end users at their request and with their permission." Mot. 33. Plaid contends that the law's intent is to criminalize phishing, which involves using fraudulent emails or websites to trick consumers into providing personal information to what appear to be legitimate companies and then using that information to facilitate identity theft and other crimes. It argues that Plaintiffs cannot plausibly allege that Plaid is not a "legitimate" company, that Plaid tricked Plaintiffs into disclosing their information, or that Plaintiffs were harmed. *Id.* at 33-34.

Neither side cites any cases analyzing section 22948.2 or setting forth the elements of a claim under that statute, and the court's own research yielded none. However, the court finds that Plaintiffs have sufficiently alleged a violation of the Anti-Phishing Act based on the plain language of the statute, which makes it unlawful to "take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Specifically, Plaintiffs assert that Plaid used the internet to induce Plaintiffs to provide their financial account credentials by representing itself to be Plaintiffs' financial institutions, including by using banks' logos and color schemes, and that this was done without the institutions' authority or approval. CFAC ¶¶ 35, 37-41, 74. They also allege that they were "adversely affected" by Plaid's actions because Plaid obtained their identifying information through deceit and used that information to access their sensitive information. *Id*. at ¶ 354.

Plaid argues that Plaintiffs must allege that Plaid acted with the goal of facilitating identity theft, but the statute imposes no such requirement. Plaid also contends that the allegation that Plaid acted without the approval or authority of the financial institutions is unsupported. Mot. 34 (citing CFAC ¶ 353). This is inaccurate. The CFAC alleges that banks have voiced concerns about the actions of data aggregators like Plaid and that some banks, including PNC bank, have taken action to prevent Plaid from accessing their banking customers' information for Venmo and other apps. CFAC ¶¶ 78-81. Moreover, Plaid's assertion that it acted with the financial institutions' approval is directly contradicted by the allegations in the December 21, 2020 PNC Complaint, in which PNC alleges that Plaid "has sought to obtain trust and consumer confidence from consumers by intentionally designing user interfaces to misleadingly suggest that Plaid was affiliated or associated with, or sponsored by, PNC" and brings claims for trademark counterfeiting, trademark infringement, false advertising, false designation of origin, and unfair competition. PNC Compl. ¶¶ 4, 44-55.

The court concludes that Plaintiffs have stated a claim under section 22948.2.

6. California Civil Code sections 1709 and 1710

Plaintiffs' ninth claim is for violation of California Civil Code sections 1709 and 1710 (deceit). Section 1709 provides that "[o]ne who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which he thereby suffers." Cal. Civ. Code § 1709. Section 1710 defines "deceit" as

> 1. The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
>
> 2. The assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true;
>
> 3. The suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or,
>
> 4. A promise, made without any intention of performing it.

Cal. Civ. Code § 1710. Plaintiffs allege that Plaid "engaged in deceit by intentionally concealing and failing to disclose its true nature and conduct to consumers." CFAC ¶ 360.

"[T]he elements of an action for fraud and deceit based on concealment are: (1) the defendant must have concealed or suppressed a material fact, (2) the defendant must have been under a duty to disclose the fact to the plaintiff, (3) the defendant must have intentionally concealed or suppressed the fact with the intent to defraud the plaintiff, (4) the plaintiff must have been unaware of the fact and would not have acted as he did if he had known of the concealed or suppressed fact, and (5) as a result of the concealment or suppression of the fact, the plaintiff must have sustained damage." *Tenet Healthsystem Desert, Inc. v. Blue Cross of California*, 245 Cal. App. 4th 821, 844 (2016) (discussing a claim for fraud based on suppression of facts under Cal. Civ. Code § 1710(3)). As to the second element, "[w]here . . . the transactions do not involve fiduciary or confidential relationships, a duty to disclose arises when:

> (1) the defendant makes representations but does not disclose facts which materially qualify the facts disclosed, or which render his disclosure likely to mislead; (2) the facts are known or accessible only to defendant, and defendant knows they are not known to or reasonably discoverable by the plaintiff; [or] (3) the defendant actively conceals discovery from the plaintiff.

Lewis v. Google LLC, 461 F. Supp. 3d 938, 960 (N.D. Cal. 2020) (quoting *Tenet*, 245 Cal. App. 4th at 844).

Plaid first points to Plaintiffs' failure to plead elements one and three of the five-part standard articulated in *Tenet.* It argues that Plaintiffs cannot plausibly allege concealment of a material fact or that Plaid intentionally concealed any fact with an intent to defraud due to the disclosures in its privacy policy. For the reasons discussed above, Plaid cannot challenge Plaintiffs' allegations about its misleading statements, actions, omissions, and nondisclosures by pointing to its privacy policy because its meaning and applicability are in dispute.

Next, Plaid asserts that Plaintiffs cannot allege a duty to disclose because there is no fiduciary relationship between the parties. Mot. 35. However, as noted above, a duty to disclose may arise in a non-fiduciary relationship under three circumstances, including where "the defendant makes representations but does not disclose facts which materially qualify the facts disclosed, or which render his disclosure likely to mislead." *See Tenet*, 245 Cal. App. 4th at 844. Plaintiffs allege that they were involved in transactions in which Plaid displayed screens that made it appear as if Plaintiffs were providing information to their financial institutions. Plaintiffs further allege that Plaid failed to adequately disclose to Plaintiffs that they were actually providing their login information to Plaid. These allegations are sufficient to plead that Plaid owed a duty to disclose the true facts about its actions to Plaintiffs.

Plaid next argues that Plaintiffs fail to plead reasonable reliance because they do not allege that they saw any statements made by Plaid, let alone that they justifiably relied on such statements. This ignores that Plaintiffs' deceit claim is premised on an omission, namely, that Plaid failed to disclose certain information that it should have disclosed. "To prove reliance on an omission, a plaintiff must show that the defendant's nondisclosure was an immediate cause of the plaintiff's injury-producing conduct." *Sloan v. Gen. Motors LLC*, 287 F. Supp. 3d 840, 873 (N.D. Cal. 2018) (quotation marks and citation omitted). "One way to do so is by simply proving that, had the omitted information been disclosed, one would have been aware of it and behaved differently." *Id.* (quotation marks and citation omitted). This "can be presumed, or at least inferred, when the omission is material." *Id*. at 874 (quotation omitted). "A misrepresentation is judged to be 'material' if 'a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question,' and as such materiality is generally a question of fact." *In re Tobacco II Cases*, 46 Cal. 4th 298, 327 (2009) (internal citations omitted). Here, Plaintiffs have alleged that had they known of Plaid's existence, role, and practices they would not have connected their financial accounts to the fintech apps the way they did. CFAC ¶¶ 105, 116, 126, 135, 145, 155, 164, 173, 183, 194, 204. The court finds that these allegations are sufficient to plead reasonable reliance.

Finally, Plaid argues that Plaintiffs fail to allege damage as required under section 1709, referring back to its argument that Plaintiffs lack Article III standing. Mot. 36 (citing Mot. 8-12). As discussed above, the court finds that Plaintiffs have sufficiently alleged injury-in-fact.

In sum, the court finds that Plaintiffs have adequately stated a claim for deceit under California Civil Code section 1709 and 1710.

United States District Court
Northern District of California

7. Unjust Enrichment

Plaintiffs' fifth claim is for unjust enrichment. "[I]n 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) (citations omitted). "When a plaintiff alleges unjust enrichment, a court may construe the cause of action as a quasi-contract claim seeking restitution." *Id.* (quotation marks and citation omitted).

Plaid argues that even if the court construes the claim as a quasi-contract claim for restitution, the claim fails because Plaintiffs have not pleaded "an actionable misrepresentation or omission." Mot. 37. As discussed above, the court concludes that Plaintiffs have adequately stated a claim for deceit. Accordingly, the motion to dismiss the unjust enrichment claim, which the court construes as a quasi-contract claim seeking restitution, is denied.

VI. CONCLUSION

For the foregoing reasons, Plaid's motion to dismiss the CFAC is granted in part and denied in part. Plaintiffs' claim for declaratory and injunctive relief, as well as their claims under the SCA, UCL, CFAA and CDAFA are dismissed with prejudice. Plaintiffs amended their complaint once already. At the hearing, the court gave Plaintiffs the opportunity to articulate any other facts that could cure the pleading defects, and this order addresses those facts. Therefore, further amendment would be futile. *See Sylvia Landfield Tr. v. City of Los Angeles*, 729 F.3d 1189, 1196 (9th Cir. 2013) ("Denial of leave to amend is not an abuse of discretion where the district court could reasonably conclude that further amendment would be futile.").

IT IS SO ORDERED.

Dated: April 30, 2021

UNITED STATES DISTRICT COURT
IT IS SO ORDERED
Judge Donna M. Ryu
NORTHERN DISTRICT OF CALIFORNIA

Donna M. Ryu
United States Magistrate Judge