UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

JAY BRODSKY, et al.,

Plaintiffs,

v.

APPLE INC.,

Defendant.

Case No. 19-CV-00712-LHK

ORDER GRANTING MOTION TO DISMISS WITH PREJUDICE

Re: Dkt. No. 46

Plaintiffs Jay Brodsky, Brian Tracey, Alex Bishop, Brendan Schwartz, William Richardson, and John Kyslowsky ("Plaintiffs") bring this putative class action against Defendant Apple Inc. ("Apple") for alleged privacy and property violations based on Apple's two-factor authentication login tool. The Court previously granted Apple's motion to dismiss the First Amended Complaint ("FAC"), but granted Plaintiffs leave to amend. ECF No. 40 ("Order"). Currently before the Court is Apple's motion to dismiss Plaintiffs' Second Amended Complaint ("SAC"). ECF No. 46 ("Mot.").[1] Because the SAC fails to cure deficiencies previously identified

[1] Apple's motion to dismiss contains a notice of motion that is separately paginated from the memorandum of points and authorities in support of the motion. Civil Local Rule 7-2(b) provides that the notice of motion and points and authorities should be contained in one document with a combined limit of 25 pages. *See* Civ. Loc. R. 7-2(b). Additionally, Apple's statement of the

in the Court's prior Order, the Court GRANTS Apple's motion to dismiss with prejudice.

I. BACKGROUND

A. Factual Background

Plaintiffs are residents of New York, California, Ohio, Pennsylvania, Colorado, and Texas. ECF No. 43 ¶ 8 ("SAC"). Apple is a California corporation that designs and sells products including iPhones, iPads, Macbooks, Apple TVs, and Apple Watches. *Id.* ¶¶ 9, 17. Once a consumer buys an Apple product, the Apple product is associated with the consumer's Apple ID, which is an individual's email address. *Id.* ¶¶ 20, 34. An Apple ID is required to use Apple services, such as FaceTime and iMessage. *Id.* ¶ 20.

Plaintiffs allege that Apple's provision of two-factor authentication ("2FA") as an Apple ID login process violates Plaintiffs' right to privacy. *Id.* ¶ 1. As in the FAC, the SAC identically alleges that 2FA is enabled in three instances: "(i) a software update occurs on one of the Apple devices; (ii) on creation of a new Apple ID; or (iii) owner of the Apple device turns on two-factor authentication in the Settings." *Id.* ¶ 35; *see also* FAC ¶ 16.

When enabled, 2FA requires a multi-step login process before a user can access Apple services. First, the user must enter his Apple ID password on the Apple device on which the user wishes to use Apple services. SAC ¶ 42. Second, the user must enter his Apple ID password on a second trusted Apple device and wait to receive a six-digit verification code on the second Apple device. *Id.* Third, the user must enter the six-digit verification code on the first Apple device. *Id.* According to Plaintiffs, 2FA takes "2-5 or more minutes" than other login processes. *Id.*; *see also* FAC ¶ 17 (pleading identical allegations).

After 2FA is enabled, Apple will sometimes send an email to the user that explains that the user can disable 2FA: "If you didn't enable two-factor authentication and believe someone else has access to your account, you can return to your previous security settings. This link and your

issues to be decided must similarly be included in the motion's pagination. *See* Civ. Loc. R. 7-2(b)(4); 7-4(a)(3). Apple's motion to dismiss also includes excessively long footnotes. One spans half a page. *See* Mot. at 10 n.5.

Apple ID security questions will expire on October 15, 2018." SAC ¶ 61; FAC ¶ 18. Plaintiffs allege that the link allowing a user to disable 2FA expires within 14 days after 2FA's enablement, and that afterwards, Plaintiffs cannot disable 2FA. SAC ¶¶ 2, 3, 61. The email also explains that 2FA "is an additional layer of security designed to ensure that you're the only person who can access your account, even if someone knows your password" and that 2FA "significantly improves the security of your Apple ID and helps protect the photos, documents, and other data you store with Apple." *Id.* ¶ 61.

Plaintiff Brodsky alleges that in September 2015, a software update enabled 2FA for Plaintiff Brodsky's Apple ID. *Id.* ¶ 37. As in the FAC, the SAC includes the exact same allegations that "Plaintiff Brodsky's Apple devices had a software update that enabled 2FA for Apple ID without his knowledge or consent on or around September of 2015." *Id.*; *see also* FAC ¶ 19.

Plaintiff Tracey alleges that "[o]n or around September 2017, 2FA was turned on for Plaintiff Tracey's Apple ID after a software update on his Apple devices." SAC ¶ 38. Specifically, Plaintiff Tracey alleges that "[h]e needs access to the latest software updates for his work," but that "Apple does not provide an option to upgrade software without 2FA." *Id.* Plaintiff Tracey, however, does not allege that he did not voluntarily consent to the software update that included enabling 2FA.

The SAC alleges that the remaining four Named Plaintiffs—Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky—"do not remember when 2FA was enabled for them." *Id.* ¶ 39. Instead, the SAC alleges the following as to the remaining four Named Plaintiffs. As to Plaintiff Bishop, the SAC alleges that on or around January 2019, "based on an unforeseen consequence outside of his control," Plaintiff Bishop "lost access to his trusted device to receive his 2FA passcode." *Id.* ¶ 48. Plaintiff Bishop could not access Apple services using Apple ID "for days." *Id.*

As to Plaintiff Schwartz, the SAC alleges that Plaintiff Schwartz lost his second trusted Apple device "based on events outside of his control." *Id.* ¶ 49. Then, Apple placed Plaintiff

Schwartz in its account recovery process and Plaintiff Schwartz could not use his Apple ID "for months." *Id.*

As to Plaintiff Richardson, the SAC alleges that Plaintiff Richardson "was locked out of [his devices] when he could not recollect offhand his password on one of the devices on or around April 2019." *Id.* ¶ 50. Plaintiff Richardson allegedly lost access to his downloaded and purchased data and spent $219.94 installing new hardware and software. *Id.*

As to Plaintiff Kyslowsky, the SAC does not include any details about when, how, or why he was locked out of his Apple devices.

Plaintiffs, however, do assert that they paid for third-party apps in "monthly, yearly, or one-time subscription[s]" and that 2FA "intercepts access to Third-Party Apps" and Apple services. *Id.* ¶¶ 21, 46, 51. According to Plaintiffs, 2FA thereby "virtually dispossesse[s]" Plaintiffs of their access to these third-party apps and Apple services for the duration of time necessary to login through 2FA. *Id.* ¶¶ 44, 46.

B. Procedural History

On February 8, 2019, Plaintiff Brodsky filed the instant case against Apple. ECF No. 1. On March 29, 2019, Plaintiffs filed the FAC, which added Tracey, Bishop, and Schwartz as named Plaintiffs. The FAC alleged five causes of action: (1) trespass to chattels, FAC ¶¶ 47-52; (2) violation of the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631, *id.* ¶¶ 53-56; (3) violation of the California Computer Crime Law ("CCCL"), California Penal Code § 502, *id.* ¶¶ 57-69; (4) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *id.* ¶¶ 70-78; and (5) unjust enrichment, *id.* ¶¶ 79-81. Plaintiffs brought suit on behalf of the following putative class:

> All persons or entities in the United States who own or owned an Apple Watch, iPhone, iPad, MacBook, or iMac or use Apple Services that have enabled two-factor authentication ("2FA"), subsequently want to disable 2FA, and are not allowed to disable 2FA.

Id. ¶ 29. The class period began "when Apple introduced 2FA in 2015." *Id.* ¶ 28.

On May 1, 2019, Apple filed a motion to dismiss Plaintiffs' FAC. ECF No. 32. On May

15, 2019, Plaintiffs filed an opposition. On May 22, 2019, Apple filed a reply in support of its motion to dismiss. ECF No. 37.

On May 15, 2019, the parties filed a joint case management statement. ECF No. 35. In the joint case management statement, Apple asked the Court to stay discovery until after the Court determines whether Plaintiffs can state a claim. *Id.* at 6. On May 16, 2019, the Court stayed discovery "until the Court orders otherwise." ECF No. 36.

On August 30, 2019, the Court granted Apple's motion to dismiss all five of Plaintiffs' causes of action. ECF No. 40 ("Order"). First, the Court dismissed Plaintiffs' claim for trespass to chattels for two reasons. *Id*. at 5-8. Plaintiffs did not adequately allege a claim for trespass to chattels because "Plaintiff [did] not allege facts to indicate that Plaintiffs failed to authorize the enablement of 2FA." *Id*. at 6. Specifically, the Court concluded that the FAC "allege[d] that 2FA is enabled when an Apple ID user voluntarily turn[ed] on 2FA, install[ed] a software update, or create[d] a new Apple ID," but that "[n]one of those means to enable 2FA permit[ted] Apple to enable 2FA unilaterally and without Plaintiffs' authorization." *Id.* Plaintiff Brodsky did not allege whether he read or reviewed the software update or "whether the message disclosed that the update would enable 2FA." *Id.* at 7. Additionally, the Court held that Plaintiffs had not alleged that any trespass harmed Plaintiffs as required under binding California Supreme Court precedent. *Id.* Rather, Plaintiffs only pleaded that "each login process [took] an additional estimated 2-5 more minutes with 2FA," and such allegations were "plainly insufficient to allege the requisite showing of harm." *Id.* In situations where Plaintiffs argued that they "suffer[ed] longer dispossessions," the Court nonetheless concluded that Apple did not proximately cause Plaintiffs' dispossession from their Apple devices or services because the FAC "d[id] not allege that Apple or 2FA led Plaintiffs to lose access to their trusted devices." *Id.* at 8. Rather, the FAC simply alleged that Plaintiffs lost access based on events "outside of [their] control." *Id.* Accordingly, the Court granted Apple's motion to dismiss Plaintiffs' trespass to chattels claim under California law. *Id.*

Second, the Court dismissed Plaintiffs' claim for violating the CIPA, again for two reasons. The Court noted that "[t]he CIPA is an anti-wiretapping statute that is violated when a person, without authorization, 'reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable.'" *Id.* at 9 (quoting Cal. Penal Code § 631(a)). The CIPA, however, "prohibit[s] only third party access to ongoing communications," and "the only communications that Plaintiffs allege Apple 'intercepted' are Plaintiff's communications to Apple." *Id.* at 9-10 (quotation marks omitted). Furthermore, the Court concluded that Plaintiffs "also failed to identify the contents of any communication that Apple allegedly intercepted, as required to state a claim under the CIPA" because Plaintiffs' "login activities," such as usernames and passwords, did not qualify as "contents" under prevailing law. *Id.* at 10-11. As a result, the Court granted Apple's motion to dismiss Plaintiffs' CIPA claim.

Third, the Court addressed Plaintiffs' claims under the federal CFAA. *Id.* at 11-14. Relying on binding Ninth Circuit precedent, the Court concluded that "the plain language of the CFAA target[s] the unauthorized procurement or alteration of information not its misuse or misappropriation," and that under the CFAA, "Plaintiffs must also plead that Apple's actions caused loss of more than $5,000 during any one-year period." *Id.* at 12 (quotation marks omitted). On this basis, the Court dismissed Plaintiffs' CFAA claims because Plaintiffs authorized 2FA through voluntary software updates. *Id.* at 13. Insofar as Plaintiffs "attempt[ed] to allege that Apple exceeded Plaintiffs' authorization," this argument also failed because Plaintiffs had not alleged that they "revoked any consent for Apple's servers to receive Plaintiffs' login activities." *Id.* at 13. Importantly, the Court noted that "Plaintiffs also d[id] not explain how Apple's access to Plaintiffs' 'login activities' via 2FA [was] at all different from Apple's access to such login activities when Plaintiffs employ a different Apple ID login method." *Id.* Finally, the Court also disposed of Plaintiffs' CFAA claims because Plaintiffs failed to plead $5,000 in damages over a one-year period. *Id.* at 14. Therefore, the Court granted Apple's motion to dismiss Plaintiffs' CFAA claims.

Fourth, the Court dismissed Plaintiffs' claims under the CCCL. *Id.* at 14-16. The Court held that "the CCCL prohibits only access or disruptions to a computer system that are 'without permission,'" and that "a defendant acted without permission . . . [when] the offending software was designed in such a way to render ineffective any barriers the Plaintiffs must wish to use to prevent access to their information." *Id.* at 15 (quotation marks omitted). Because Plaintiffs did not offer any allegations about how Plaintiffs attempted to prevent 2FA's access to their information, Plaintiffs' CCCL claims failed. *Id.* Additionally, Plaintiffs' CCCL claims failed because the FAC "merely parrot[ed] the language of the CCCL," and such "boilerplate allegations also provide[d] a reason to dismiss Plaintiffs' CCCL claims." *Id.* at 15-16. As a result, the Court granted Apple's motion to dismiss Plaintiffs' CCCL claims.

Fifth, the Court analyzed Plaintiffs' unjust enrichment claim under California law. *Id.* at 16-17. California law, however, "does not recognize a separate cause of action for unjust enrichment." *Id.* at 16 (citation omitted). Though "courts have [sometimes] construed purported claims for unjust enrichment as quasi-contract claims seeking restitution," "Plaintiffs' FAC include[d] no allegation that Apple is liable in quasi-contract." *Id.* at 16-17. Therefore, the Court granted Apple's motion to dismiss Plaintiff's unjust enrichment claims.

Sixth, in the alternative, the Court found that Plaintiffs' claims under the CIPA, CFAA, and CCCL were time-barred. *Id.* at 17-19. "The longest applicable statute of limitations [was] three years," but Plaintiffs only brought suit "approximately three and a half years after Plaintiff Brodsky alleges that he enabled 2FA on his Apple devices." *Id.* at 17. Additionally, the continuous accrual doctrine, the continuing violation doctrine, and the delayed discovery rule did not apply and thus did not save Plaintiffs' CIPA, CFAA, and CCCL claims. *Id.* at 18-19.

Finally, as to Plaintiffs' common law claims—namely the trespass to chattels and unjust enrichment claims—the Court found that the FAC failed to satisfy Rule 8. *Id.* at 20. Specifically, Plaintiffs had not alleged their states of residence or which state's law applied to each of Plaintiffs' common law claims such that "Apple [could not] adequately defend itself, nor [could] the Court assess the sufficiency of Plaintiffs' claims." *Id.* The Court directed Plaintiffs to "amend their pleading to specify their states of residence and clarify under which state's common law Plaintiffs bring their trespass to chattels and unjust enrichment claims." *Id.* The Court also noted that "[f]ailure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice. *Id.*

On September 26, 2019, Plaintiffs filed the SAC. ECF No. 43. The SAC adds two new Named Plaintiffs, William Richardson and John Kyslowsky, who are residents of Colorado and Texas respectively. *Id.* ¶ 8. The SAC also alleges that Plaintiff Brodsky is a New York resident, Plaintiff Tracey is a California resident, Plaintiff Bishop is an Ohio resident, and Plaintiff Schwartz is a Pennsylvania resident. *Id*. Additionally, the SAC alleges that California law applies to all of Plaintiffs' claims based on a choice of law provision in Apple's terms and use agreements. *Id.* ¶ 15; *see also id.* ¶ 76 ("California's substantive laws including common law apply to every member of the Class, regardless of where in the United States the Class Member resides based on Apple's 'Controlling Law' provisions in its Terms and Conditions agreements for all of its products and services."). The SAC also alleges that Plaintiffs' states of residence "have the substantively same laws for common law claims at issue here, *i.e.*, trespass of [sic] chattels and unjust enrichment claims," such that "applying California law for common law claims is appropriate here because the differences of application will not be substantive." *Id.* ¶ 77.

Additionally, the SAC now pleads that Plaintiffs pay for third-party apps in "monthly, yearly, or one-time subscription[s]." *Id.* ¶ 21. Plaintiffs also assert that 2FA "intercepts access to Third-Party Apps" and Apple services, *id.* ¶¶ 46, 51, just as Plaintiffs previously argued that "Apple has 'intercepted' the user's communication with the Apple service," Order at 11; *see id.* ("However, if a user cannot access an Apple service like FaceTime due to 2FA, as Plaintiffs allege, the user cannot create any communication over FaceTime for Apple to 'intercept.'"). The SAC also adds a new allegation that "[b]y filing . . . this lawsuit, Plaintiffs hereby revoke any authorization Apple may have to continue to operate 2FA on Apple Devices." *Id.* ¶ 65.

Based on these allegations, the SAC realleges the same five causes of action as the FAC: (1) trespass to chattels, *id.* ¶¶ 94-100; (2) violation of the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631, *id.* ¶¶ 101-05; (3) violation of the California Computer

Crime Law ("CCCL"), California Penal Code § 502, *id.* ¶¶ 106-18; (4) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *id.* ¶¶ 119-128; and (5) unjust enrichment, *id.* ¶¶ 129-33. Plaintiffs again bring suit on behalf of the following putative class:

> All persons or entities in the United States who own or owned an Apple Watch, iPhone, iPad, MacBook, or iMac or use Apple Services that have enabled two-factor authentication ("2FA"), subsequently want to disable 2FA, and are not allowed to disable 2FA.

Id. ¶ 71. The class period began "when Apple introduced 2FA in 2015." *Id.* ¶ 70. In the SAC, Plaintiffs again seek to represent subclasses as in the FAC. *Id.* ¶¶ 72-73. The SAC, however, includes a new subclass whereby Plaintiffs Richardson and Kyslowsky seek to represent an analogous subclass of "senior persons in the United States." *Id.* ¶ 74.

On October 22, 2019, Apple filed the instant motion to dismiss Plaintiff's SAC. ECF No. 46 ("Mot."). On November 5, 2019, Plaintiffs filed an opposition. ECF No. 47 ("Opp."). On November 19, 2019, Apple filed a reply. ECF No. 50 ("Reply").

II. LEGAL STANDARD

A. Motion to Dismiss Under Federal Rule of Civil Procedure 12(b)(6)

Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). The United States Supreme Court has held that Rule 8(a) requires a plaintiff to plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St.*

Paul Fire & Marine Ins. Co., 519 F.3d 1025, 1031 (9th Cir. 2008). The Court, however, need not "assume the truth of legal conclusions merely because they are cast in the form of factual allegations." *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (internal quotation marks omitted). Additionally, mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Leave to Amend

If the Court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Id.* at 1130 (internal quotation marks omitted). Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008). At the same time, a court is justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *See Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892 (9th Cir. 2010). Indeed, a "district court's discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint." *Cafasso, U.S. ex rel. v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1058 (9th Cir. 2011) (quotation marks omitted).

III. DISCUSSION

Apple moves to dismiss each of Plaintiffs' claims for failure to state a claim. Apple also contends that certain claims are fail to satisfy Rule 8's pleading standard or are barred by the statute of limitations. The Court first addresses the sufficiency of each of Plaintiffs' individual claims before turning to Apple's other arguments.

A. Claim for Trespass to Chattels

Plaintiffs allege that Apple committed trespass to chattels because Apple "interfered with Plaintiffs and Class Members' possessory interest of their one or more Apple devices by requiring an extraneous login process through two-factor authentication that is imposed on Plaintiffs and Class members without authorization or consent." SAC ¶ 96.

As an initial matter, the Court notes that the SAC alleges that California law applies to all of Plaintiffs' claims based on a choice of law provision in Apple's terms and use agreements. *Id.* ¶ 15; *see also id.* ¶ 76 ("California's substantive laws including common law apply to every member of the Class, regardless of where in the United States the Class Member resides based on Apple's 'Controlling Law' provisions in its Terms and Conditions agreements for all of its products and services.").

For Plaintiffs' common law claims—namely their claims for trespass to chattels and unjust enrichment—Plaintiffs allege that they bring those claims under the common law of New York, Ohio, Pennsylvania, Colorado, and Texas "[i]n the alternative." *Id.* ¶¶ 95, 130. However, the SAC also alleges that Plaintiffs' states of residence "have the substantively same laws for common law claims at issue here, *i.e.*, trespass of [sic] chattels and unjust enrichment claims," such that "applying California law for common law claims is appropriate here because the differences of application will not be substantive." *Id.* ¶ 77.

Furthermore, in any event, Apple argues in its motion to dismiss that Plaintiffs' common law claims must be dismissed insofar as those claims rely on non-California law. *See* Mot. at 10 n.5, 24 n.7. Plaintiffs do not respond to Apple's arguments, and as such, Plaintiffs have abandoned their common law claims premised on non-California law. *Moore v. Apple, Inc.*, 73 F. Supp. 3d 1191, 1205 (N.D. Cal. 2014) (stating that a failure in an opposition to address arguments raised in a motion to dismiss constitutes abandonment of the claim, which results in dismissal with prejudice). Accordingly, the Court proceeds to analyze Plaintiffs' common law claims under

California law.

Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003). To state a trespass to chattels claim, a plaintiff must plead that "(1) the defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use[] proximately caused damage." *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 842 (N.D. Cal. 2017) (quoting *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069-70 (N.D. Cal. 2000)).

As with the previous motion to dismiss, Apple argues that (1) Apple did not enable 2FA without Plaintiffs' authorization; and (2) Plaintiffs have not alleged that Apple damaged Plaintiffs. The Court addresses each argument in turn.

1. Plaintiffs Have Not Alleged that 2FA was Enabled Without Plaintiffs' Authorization

First, Apple contends that Plaintiffs consented to 2FA, and thus, that any interference with possession was authorized. Under *Hamidi*, a trespass only occurs where an interference is "unauthorized." 30 Cal. 4th at 1350. Plaintiffs make much of their new allegation that "[b]y filing . . . this lawsuit, Plaintiffs hereby revoke any authorization Apple may have to continue to operate 2FA on Apple Devices." *Id.* ¶ 65. However, as the Court noted in its prior Order, courts consistently hold that in the context of a software update and digital trespass, "[v]oluntary installation runs counter to the notion that the alleged act was a trespass." *In re Apple & ATTM Antitrust Litig.*, 2010 WL 3521965 (N.D. Cal. July 8, 2010), *vacated in part sub nom. on other grounds In re Apple & AT & TM Antitrust Litig.*, 826 F. Supp. 2d 1168 (N.D. Cal. 2011); *see* Order at 6. Plaintiffs do not point to any case law or authority to the contrary.

As a result, what the Court is left with are the same allegations that were previously found wanting in the Court's prior Order. Here, Plaintiffs again do not allege facts that Plaintiffs failed to authorize the enablement of 2FA. Rather, just like the FAC, the SAC identically alleges that 2FA is enabled in three instances: when an Apple ID user voluntarily turns on 2FA, installs a software update, or creates a new Apple ID. SAC ¶ 35; FAC ¶ 16. As the Court previously concluded, "[n]one of those means to enable 2FA permits Apple to enable 2FA unilaterally and without Plaintiffs' authorization." *Id.* at 6.

Plaintiffs nevertheless persist and argue that they had "no notice of [the] 2FA feature upgrade." Opp. at 6. To be sure, as the Court noted in its prior Order, courts have recognized that "consent to enter may be limited and that a trespass claim may lie when the scope of consent is exceeded." *In re Apple Inc. Device Performance Litig.* ("*In re Apple*"), 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018). However, in *In re Apple*, the plaintiffs' complaint quoted the message that accompanied Apple's software update and explained how the message failed to identify additional effects of the software update. *Id.* The *In re Apple* plaintiffs did not consent to those additional effects of the software update.

Here, as before, the SAC offers no information about Plaintiff Brodsky's 2015 software update that allegedly enabled 2FA on his phone, nor about whether Plaintiff Brodsky read or reviewed the message that accompanied the update and whether the message disclosed that the update would enable 2FA. *Id.* ¶ 37. Nor has Plaintiff Tracey alleged any facts related to his alleged involuntary enablement of 2FA through voluntary software updates. *Id.* ¶ 38. Plaintiffs' bald assertions in the SAC that they did not consent to enabling 2FA is a legal conclusion not entitled to the presumption of truth. *See In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (holding that a court need not accept as true "allegations that are merely conclusory"). Indeed, none of the remaining Named Plaintiffs—Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky—even specify how they enabled 2FA on their Apple devices. *Id.* ¶ 39. Accordingly, Plaintiffs have not alleged that 2FA was enabled without Plaintiffs' authorization.

2. Plaintiffs Have Not Alleged That Any Trespass Harmed Them

Second, Plaintiffs' claim for trespass to chattels fails because Plaintiffs have again failed to allege that Apple harmed Plaintiffs through 2FA. The California Supreme Court has explained that, "while a harmless use or touching of personal property may be a technical trespass (see Rest. 2d of Torts, § 217), an interference (not amounting to dispossession) is not actionable under modern California and broader American law without a showing of harm." *Intel Corp.*, 30 Cal. 4th at 1350-51. In the context of a trespass to a computer system, a plaintiff must allege "that the purported trespass: (1) caused physical damage to the personal property, (2) impaired the condition, quality, or value of the personal property, or (3) deprived plaintiff of the use of personal property for a substantial time." *Fields v. Wise Media, LLC*, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24, 2013).

Plaintiffs argue that the SAC adequately alleges harm because Plaintiffs are "blocked 100%" for "ongoing short periods of time when 2FA is triggered" or "when not connected to the internet" and because they are "lock[ed] out for days . . . when access to a trusted device to receive 2FA is lost." Opp. at 8. However, as in the FAC, the SAC only alleges that 2FA takes "2-5 or more minutes" than other login processes. SAC ¶ 42.

Plaintiffs' allegations are insufficient to allege the requisite showing of harm. In *In re iPhone Application Litigation*, this Court concluded that Apple programs that consumed the devices' memory and "shortened the[ir] battery life" were insufficient to state a claim. 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012). The allegations did not suggest that Apple's trespass "caused an interference with the intended functioning" of the devices. *Id.*; *see also Hamidi*, 30 Cal. 4th at 1347 (holding that trespass to chattels "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning").

In the instant case, as the Court previously held, a delay of 2-5 minutes does not impair the functioning of Plaintiffs' Apple devices or Apple IDs. Order at 7; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1069; *Hamidi*, 30 Cal. 4th at 1347. Plaintiffs do not allege that 2FA prevents Plaintiffs from logging in after that delay, or that Plaintiffs' devices are "damaged" by the delay. *See Engle v. Unified Life Ins. Co., Inc.*, 2014 WL 12508347, at *7 (S.D. Cal. Oct. 27, 2014) (concluding that impairment of devices for the "duration of a phone call" did not qualify as harm sufficient to state a trespass to chattels claim).

Furthermore, as recognized in the Court's earlier Order, insofar as Plaintiffs contend that

Plaintiffs suffer longer dispossessions, any such allegations fail to adequately allege proximate causation. Order at 8. Plaintiffs offer no new argument as to how their pleading adequately alleges proximate causation. Instead, the SAC includes the same or nearly identical allegations as the FAC, and Plaintiffs fail to allege that Apple or 2FA led Plaintiffs to lose access to their trusted devices. Rather, Plaintiff Bishop lost access to his trusted device "based on an unforeseen consequence outside of his control," and Plaintiff Schwartz lost access to his trusted device "based on events outside of his control." SAC ¶¶ 48-49. As to Plaintiff Richardson, the SAC alleges that he "was locked out of [his devices] when he could not recollect offhand his password on one of the devices on or around April 2019." *Id.* ¶ 50. In none of these instances did Apple or 2FA cause Plaintiffs' dispossession from their Apple devices and Apple services. *See Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566 (1996) (holding that a trespass to chattels occurs only where the interference "has proximately caused injury"). Thus, Plaintiffs have not adequately alleged a claim for trespass to chattels.

Therefore, the Court GRANTS Apple's motion to dismiss Plaintiffs' claim for trespass to chattels. Plaintiffs failed to cure the same deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 5-8. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs' claim for trespass to chattels was deficient for the same exact reasons as stated in this Order. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' claim for trespass to chattels with prejudice.

B. Claim for Violation of the California Information Privacy Act ("CIPA")

The Court next addresses Plaintiffs' CIPA claim. Plaintiffs allege that Apple violated the CIPA because via 2FA, "Apple, by injecting itself in the process by requiring extra logging [sic] steps, has acquired without authorization confidential electronic communication owned by

Plaintiffs and Class Members." SAC ¶ 102.

The CIPA is an anti-wiretapping statute that is violated when a person, without authorization, "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." Cal. Penal Code § 631(a). The CIPA was "passed to protect against the invasion of privacy," *Matera v. Google Inc.*, 2016 WL 5339806, at *10 (N.D. Cal. Sept. 23, 2016), and requires the "interception of an electronic communication," *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006).

In the instant case, Plaintiffs contend that 2FA violates Plaintiffs' privacy rights under the CIPA. Apple responds that (1) the CIPA prohibits only a third party's interceptions and that Apple is not a third party; and (2) Plaintiffs fail to allege the contents of any communications that Apple intercepted. The Court addresses each argument in turn.

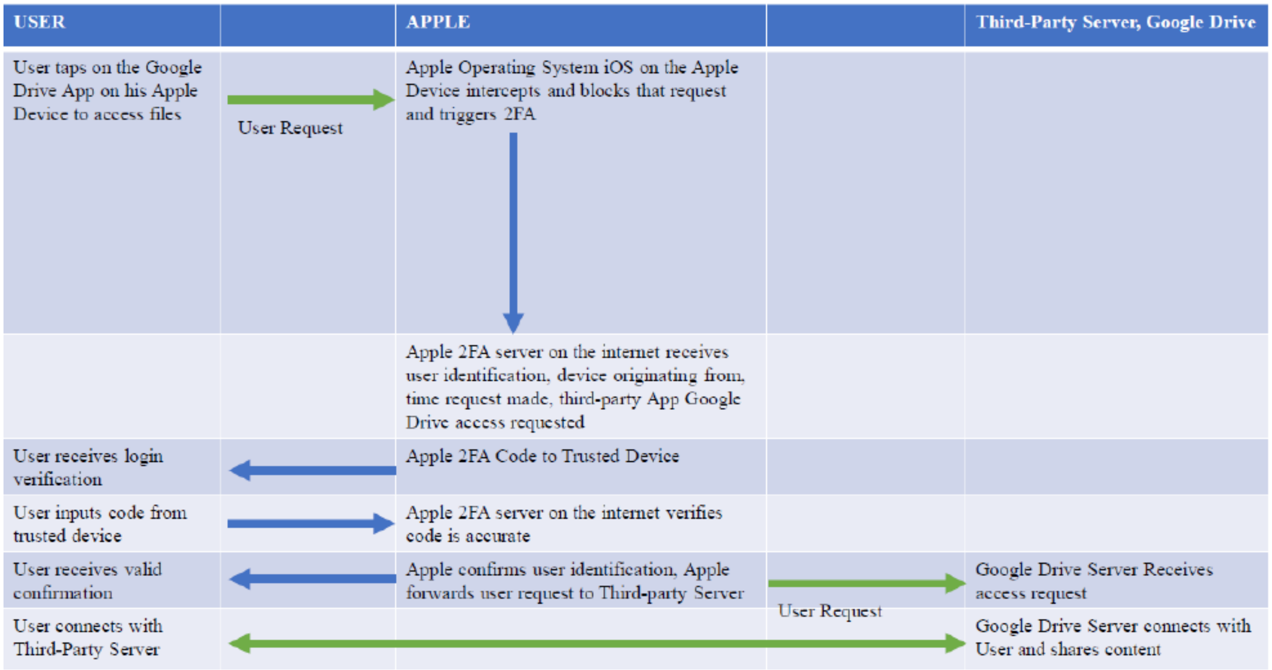
1. Plaintiffs Have Failed To Allege That Apple Was Not A Party To The Communications

Courts have interpreted the CIPA to prohibit only "third party access to ongoing communications." *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017). In *In re Facebook*, the district court held that Facebook could not "intercept" communications to which Facebook was already a party. *Id.* at 844-45; *see Thomasson v. GC Servs. Ltd. P'Ship*, 321 F. App'x 557, 559 (9th Cir. 2008) (explaining that California courts interpret the anti-eavesdropping provision of the CIPA "to refer to a third party secretly listening to a conversation between two other parties").

Plaintiffs disagree and argue that CIPA liability attaches "irrespective of whether Apple is a party." Opp. at 11. Plaintiffs again rely on *Ramos v. Capitol One, N.A.*, 2017 WL 3232488 (N.D. Cal. July 27, 2017), *id*. at 12, which the Court previously distinguished, Order at 10. In *Ramos*, the district court concluded that a defendant could be liable for intercepting a communication between two other parties on the defendant's phone lines. 2017 WL 3232488, at *9. *Ramos* is inapplicable to the instant case, in which Plaintiffs' "login activities" are communications that Plaintiffs send to Apple's servers.

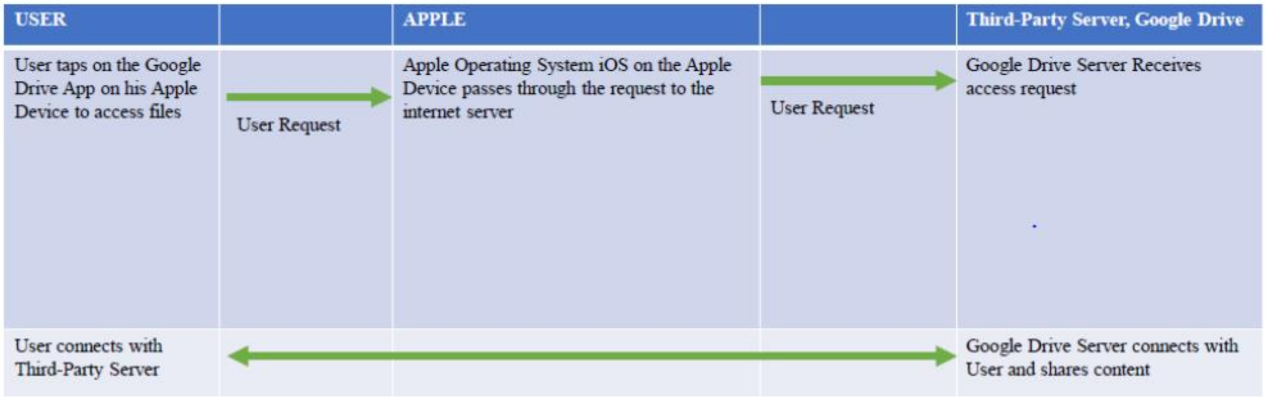
In the alternative, Plaintiffs contend that Apple is not a party to Plaintiffs' communications. *Id*. Plaintiffs, however, do not cite to any allegations in the SAC for this argument. Instead, Plaintiffs simply point to two tables that appear only in their opposition brief. Opp. at 11-12. Plaintiffs assert that these two tables allegedly demonstrate that Apple is not a party to Plaintiffs' communications. The tables are reproduced below:

Table 2: Steps showing Plaintiff access Google Drive Server with Apple 2FA Enabled



USER		APPLE		Third-Party Server, Google Drive
User taps on the Google Drive App on his Apple Device to access files	→ User Request	Apple Operating System iOS on the Apple Device intercepts and blocks that request and triggers 2FA ↓		
		Apple 2FA server on the internet receives user identification, device originating from, time request made, third-party App Google Drive access requested		
User receives login verification	←	Apple 2FA Code to Trusted Device		
User inputs code from trusted device	→	Apple 2FA server on the internet verifies code is accurate		
User receives valid confirmation	←	Apple confirms user identification, Apple forwards user request to Third-party Server	→ User Request	Google Drive Server Receives access request
User connects with Third-Party Server	↔			Google Drive Server connects with User and shares content

Table 3: Steps showing Plaintiff access Google Drive Server with Apple 2FA Disabled



USER		APPLE		Third-Party Server, Google Drive
User taps on the Google Drive App on his Apple Device to access files	→ User Request	Apple Operating System iOS on the Apple Device passes through the request to the internet server	→ User Request	Google Drive Server Receives access request
User connects with Third-Party Server	↔			Google Drive Server connects with User and shares content

Even if the Court considers Tables 2 and 3, which are not pleaded in the SAC, the Court nonetheless concludes that Plaintiffs fail to allege that Apple was a third party to Plaintiffs' communications. Table 2 allegedly shows what happens when users attempt to access a third-party app with 2FA enabled. Table 3 purportedly shows what happens when users attempt to access a third-party app with 2FA disabled. However, regardless of whether 2FA is enabled or disabled, users must still communicate with Apple, who "passes through the [user's] request" to the third-party app. Opp. at 12 (Table 3). Nothing in Tables 2 or 3 suggest that Apple is a third party to communications. Instead, Tables 2 and 3 confirm that the only communications that Plaintiffs argue Apple "intercepted" are Plaintiffs' communications to Apple. As in *In re Facebook*, Apple cannot intercept communications to which Apple is already a party. Thus, Plaintiffs have not alleged a violation of the CIPA.

2. Plaintiffs Have Failed To Allege The Contents Of Any Intercepted Communication

Second, Plaintiffs have also failed to identify the contents of any communication that Apple allegedly intercepted, as required to state a claim under the CIPA. *See* Cal. Penal Code § 631(a) (prohibiting unauthorized access of the "contents" of any communication). "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) (citation omitted).

Under the Wiretap Act, the term "contents" is defined as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510. The Ninth Circuit has held that "record information regarding the characteristics of the message that is generated in the course of the communication" does not qualify as "contents." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Record information, the Ninth Circuit explained, "includes the name, address, and subscriber number or identity of a subscriber or customer." *Id.* (quotation marks omitted). Accordingly, text messages qualify as contents under the Wiretap Act. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083 (N.D. Cal. 2015). However, user names, passwords, and geographic location information are not contents. *Id.* at 1082, 1084.

In the instant case, Plaintiffs allege that Apple intercepted Plaintiffs' "requests" to "access to Third-Party Apps" or presumably Plaintiffs' user names and passwords. SAC ¶¶ 51-52. However, as the Ninth Circuit has concluded, a CIPA claim cannot be predicated on such record information. *In re Zynga Privacy Litig.*, 750 F.3d 1098 at 1106 (holding that "record information regarding the characteristics of the message that is generated in the course of the communication" does not qualify as "contents"). Indeed, *In re Carrier IQ* explicitly held that user names and passwords do not constitute "contents" under the Wiretap Act. 78 F. Supp. 3d at 1082, 1084.

Additionally, in the Court's prior Order, the Court rejected Plaintiffs' argument that when 2FA prevents a user from accessing his Apple ID or services (such as when the user has lost his trusted device), Apple has "intercepted" the user's communication with the Apple service. Order at 11. The Court explained that "if a user cannot access an Apple service like FaceTime due to 2FA, as Plaintiffs allege, the user cannot create any communication over FaceTime for Apple to 'intercept.'" Order at 11. Plaintiffs recycle that same argument in the SAC, but also allege that "[o]n information and belief, Apple also uses its 2FA to intercept content, such as photos, music and other files on Apple devices stored locally" and on third-party apps. SAC ¶ 51. This allegation, however, contradicts the other allegations in the SAC.

First, the SAC's allegation that Apple "uses its 2FA to intercept content, such as photos, music and other files on Apple devices stored locally" is incorrect. The SAC alleges that 2FA is simply a process for logging into an Apple ID, which is a separate process from accessing "files on Apple devices stored locally." *Id.* ¶¶ 3, 51.

Second, in any event, Plaintiffs clarify in their opposition brief that the "photos, music[,] and other files . . . stored locally" are not in fact stored locally. Instead, Plaintiffs clarify that "photos, music[,] and other files . . . stored locally" actually refers to content in Apple Services and third-party apps. *See* Opp. at 12 ("SAC lists out and gives examples of different Apple Services and Third-Party Apps used by Plaintiffs. Undisputedly, these Apps and Services include Content. For example, Google drive includes files, photos with content hosted by third party, Google Servers." (citations omitted)). However, as the SAC alleges elsewhere, Apple's "intercepts access to Third-Party Apps" and Apple Services and "intercepts such requests and communications by interjecting 2FA in the process . . . when opening a Third-Party App" or Apple Services. *Id.* ¶¶ 51-52. As the Court previously held, "if a user cannot access a [service] like FaceTime [or other third-party apps] due to 2FA, as Plaintiffs allege, the user cannot create any communication . . . for Apple to 'intercept.'" Order at 11. Therefore, just as in the FAC, the SAC fails to allege the contents of any communication that Apple intercepted.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CIPA claim. Plaintiffs failed to cure the same deficiencies the Court previously identified in its prior Order, and any new allegations fail to justify a different conclusion. Order at 9-11. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho,* 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs' CIPA claim was deficient for the same exact reasons as stated in this Order. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CIPA claim with prejudice.

C. Claims for Violation of the Computer Fraud and Abuse Act ("CFAA")

Next, the Court discusses Plaintiffs' claims under the federal CFAA. Plaintiffs allege that Apple "intentionally accessed through the 2FA feature Plaintiffs' and Class Members' computers" and that Apple "knowingly caused the transmission of information, i.e. sending and receiving of six-digit verification code [sic] on another device." SAC ¶¶ 120-21. Plaintiffs bring claims under two provisions of the CFAA, 18 U.S.C. § 1030(a)(2) and 18 U.S.C. § 1030(a)(5). *Id.*

The CFAA is an anti-hacking statute that creates liability where a defendant "intentionally accesses a computer without authorization or exceeds authorized access," and thus obtains "information from any protected computer" or financial records. 18 U.S.C. § 1030(a)(2). The CFAA also creates liability for "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." *Id.* § 1030(a)(5)(A)(i). Thus, "the plain language of the CFAA target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (alteration in original) (citation omitted). Based on the SAC's allegations, the CFAA requires that Plaintiffs also plead that Apple's actions caused a loss of more than $5,000 during any one-year period. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131-32 (9th Cir. 2009) (citing 18 U.S.C. § 1030(a)).

Finally, the CFAA was enacted "primarily to address the growing problem of computer hacking," such that the en banc Ninth Circuit has favored an interpretation of the statute that "maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate." *Nosal*, 676 F.3d at 858. Given that instruction, the Court previously noted that it was "exceedingly skeptical of Plaintiffs' theory that 2FA—an Apple login method that according to Plaintiffs' FAC 'significantly improves the security of [a user's] Apple ID'—can render Apple liable under the CFAA, particularly given Plaintiffs' vague and conclusory allegations." Order at 12.

Plaintiffs' amendments in the SAC have done little to dispel that skepticism. At base, Plaintiffs' SAC alleges a claim that 2FA slows down the login process, not a hacking claim. As the Court previously noted, "[a]llowing CFAA claims to proceed on such conclusory, thin allegations 'would expand the CFAA too far.'" Order at 13-14 (quoting *In re Apple*, 347 F. Supp. 3d at 453)). As a result, the Court again agrees with Apple that Plaintiffs have failed to plead that (1) Apple hacked into Plaintiffs' devices without authorization; and (2) any Apple actions caused $5,000 in damages in any given one-year period. The Court addresses each argument in turn.

1. Plaintiffs Have Not Alleged That Any Access Was Unauthorized

First, both CFAA provisions under which Plaintiffs bring their claims apply only where a defendant accesses or transmits a program to a computer "without authorization" or by "exceeding authorized access." "'[A]uthorization,'" however, in the CFAA context, "is most naturally read in reference to the *identity* of the person accessing the computer or website, not *how* access occurs."

hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019) (emphasis in original). Therefore, if a plaintiff authorizes an individual to access the plaintiff's computer, the plaintiff's CFAA claim cannot be based simply on the manner or means by which the individual accesses the computer. *See id.*; *see also Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1176-77 (C.D. Cal. 2018) (dismissing CFAA and CCCL claims because Ticketmaster "never withdrew" authorization to access its website where "Ticketmaster's cease-and-desist letter only expressed its disapproval of the method by which Defendants accessed the website"). In situations where a plaintiff clearly revokes access to a party and not simply the means, manner, or method for such access, that party may be liable under the CFAA. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1068-69 (9th Cir. 2016) (affirming CFAA liability because "Facebook explicitly revoked authorization for *any* access" (emphasis in original)).

Plaintiffs do not offer any response to this argument in their opposition brief. *See* Opp. at 13-14. As such, Plaintiffs have abandoned their CFAA claims. *Moore*, 73 F. Supp. 3d at 1205 (stating that a failure in an opposition to address arguments raised in a motion to dismiss constitutes abandonment of the claim, which results in dismissal with prejudice). Even had Plaintiffs responded, the SAC only purports to revoke Apple's authorization for the method of access, 2FA, but does not disclaim Apple's access through other Apple ID login methods. SAC ¶ 65; *hiQ Labs*, 273 F. Supp. 3d at 1113 ("'[A]uthorization,' . . . is most naturally read in reference to the *identity* of the person accessing the computer or website, not *how* access occurs."); *Ticketmaster*, 306 F. Supp. 3d at 1176-77 (dismissing CFAA and CCCL claims because Ticketmaster "never withdrew" authorization to access its website where "Ticketmaster's cease-and-desist letter only expressed its disapproval of the method by which Defendants accessed the website"). Indeed, the Court previously recognized that Plaintiffs were simply attempting to challenge Apple's method of access to Plaintiffs' login activities. Order at 13 ("Plaintiffs also do not explain how Apple's access to Plaintiffs' 'login activities' via 2FA is at all different from Apple's access to such login activities when Plaintiffs employ a different Apple ID login method."); *id.* at 10 ("[O]ther Apple ID login methods presumably also require Plaintiffs to communicate with Apple's servers."). Therefore, beyond Plaintiffs' failure to respond to Apple's argument, the SAC only challenges how access occurs through 2FA and still permits Apple to access Plaintiffs' login activities through other means, which Plaintiffs authorized. Accordingly, Plaintiffs' CFAA claims fail.

2. Plaintiffs Have Also Failed to Plead $5,000 in Damages

Second, Plaintiffs have again failed to plead the requisite damages under the CFAA. Plaintiffs contend that the SAC adequately alleges damages to satisfy the CFAA's $5,000 requirement by "list[ing] the number of [A]pple devices owned, [A]pple services subscriptions[,] and access to third-party apps that are constructively disp[ossessed]." Opp. at 14. However, Plaintiffs cannot rely on these allegations regarding the full cost of their devices and services subscriptions because the gravamen of the SAC is that 2FA adds only an "additional estimated 2-5 or more minutes" to log in with Apple ID. SAC ¶ 42. Insofar as the SAC alleges that some Plaintiffs could not access Apple services or third-party apps for longer periods of time, Plaintiffs acknowledge that they either forgot their passwords or that they were locked out based on "events outside [their] control," which cannot be attributed to Apple. *Id.* ¶¶ 48-50. Without more, the SAC does not adequately plead how Plaintiffs' damages based on their devices, Apple services subscriptions, or third-party apps for 2-5 minutes satisfy the CFAA's $5,000 loss during a one-year period requirement.

Plaintiffs' only remaining damages allegation is that "Apple has collected personal information that has economic value to the Plaintiffs and Class Members, the unauthorized collection of which resulted in the deprivation or diminution of such economic value, causing Plaintiffs and Class Members to sustain . . . economic loss with an aggregated value of at least $5,000 during a one-year period." *Id.* ¶ 126. Plaintiffs, however, do not rely on this allegation in their opposition, and for good reason. *See* Opp. at 13-14.

Recently, the Ninth Circuit decided a CFAA case where Plaintiffs' "theory of loss [was] that he and his fellow class members were denied the profits they might have received from commodifying the personal information that [the defendant] allegedly obtained through unlawful means." *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262 (9th Cir. 2019). The plaintiff in *Andrews* 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." *Id.* The Ninth Circuit rejected Plaintiff's theory of loss because the CFAA's "narrow conception of 'loss' . . . does not include a provision that aligns with [plaintiff's] theory." *Id.* *Andrews* therefore forecloses Plaintiffs' theory that Apple caused Plaintiffs' and Class Members damages in the form of lost economic value in their personal information. As a result, Plaintiffs have failed to plead $5,000 in damages.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CFAA claims. Plaintiffs failed to cure the same or similar deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 11-14. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs' CFAA claims were deficient for the same or similar reasons as stated in this Order. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CFAA claims with prejudice.

D. Claims for Violation of the California Computer Crime Law ("CCCL")

Next, the Court discusses Plaintiffs' claims under the CCCL, Cal. Penal Code § 502. The CCCL is also sometimes referred to as the California Comprehensive Computer Data Access and Fraud Act and abbreviated as "CDAFA." *Facebook, Inc. v. Grunin*, 77 F. Supp. 3d 965, 971 (N.D. Cal. 2015); *Oracle USA, Inc. v. Rimini St., Inc.*, 879 F.3d 948, 952 (9th Cir.), *cert. granted*, 139 S. Ct. 52 (2018), and *rev'd in part*, 139 S. Ct. 873 (2019).

Plaintiffs bring claims under five provisions of the CCCL, Cal. Penal Code §§ 502(c)(1), (3)-(5), and (7). SAC ¶¶ 109-13. For each claim, Plaintiff alleges that Apple "knowingly and without permission" accessed, altered, or otherwise disrupted Plaintiffs' Apple devices. *Id*. Case law suggests that Plaintiffs' CCCL claims rise or fall with Plaintiffs' CFAA claims because "the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA," except in terms of damages. *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010). Unlike the CFAA, the CCCL does not impose a minimum of $5,000 in damages. *Cline*, 329 F. Supp. 3d at 1052.

Like the CFAA, the CCCL prohibits only access or disruptions to a computer system that are "without permission." This means that, like a CFAA claim, a CCCL claim cannot be based simply on the method by which a defendant accesses a computer if the defendant otherwise has authorization to access the computer. As the Ninth Circuit held, "taking data using a *method* prohibited by the applicable terms of use, when the taking itself generally is permitted, does not violate the [CCCL]." *Oracle USA*, 879 F.3d at 962 (emphasis in original). In *Oracle USA*, the Ninth Circuit noted that "Oracle obviously disapproved of the method . . . by which Rimini took Oracle's proprietary information. But the key to the [CCCL] is whether Rimini was authorized in the first instance to take and use the information that it downloaded." *Id.*; *see also Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1176-77 (C.D. Cal. 2018) (dismissing CFAA and CCCL claims because Ticketmaster "never withdrew" authorization to access its website where "Ticketmaster's cease-and-desist letter only expressed its disapproval of the method by which Defendants accessed the website"). As the Court noted previously, *see supra* Part III.C.1, the SAC only purports to revoke Apple's authorization for the method of access through 2FA without disclaiming Apple's access to Plaintiffs' login activities through other means. SAC ¶ 65. In addition, the Court's prior Order also explained that Plaintiffs' CCCL claims failed in part because "Plaintiffs offer no allegations about . . . how 2FA offers Apple access to Plaintiffs' information that is somehow different from Apple's access through other Apple ID login methods." Order at 15. As a result, because the SAC only challenges the login method of 2FA without alleging that Apple is otherwise accessing Plaintiffs' login activities without authorization, Plaintiffs' CCCL claims fail.

Furthermore, Plaintiffs' CCCL claims fail for an additional reason. As the Court previously held, "Plaintiffs' specific CCCL claims all merely parrot the language of the CCCL." Order at 15. As before, the SAC includes the same exact allegations that the Court previously found insufficient in the FAC. Plaintiffs allege that "Apple knowingly and without permission has used and caused to be used Plaintiffs' and Class Members' Apple Services and Third-Party Apps configured on their Apple devices." SAC ¶ 110; FAC ¶ 61. This allegation mirrors the language of California Penal Code § 502(c)(5), which renders liable a defendant who "[k]nowingly and without permission uses or causes to be used computer services." Cal. Penal Code § 502(c)(5). Plaintiffs have simply inserted their Apple services and third-party apps in place of "computer services." For example, the SAC includes no factual allegations about how it is even possible for Apple to "use" a third-party app on Plaintiffs' devices—particularly if Plaintiffs' are "locked" out of their devices. These boilerplate allegations also provide a reason to dismiss Plaintiffs' CCCL claims. *See Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1090 (N.D. Cal. 2018) (granting a motion to dismiss where plaintiffs made only "boilerplate allegations" of CCCL violations).

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CCCL claims. Plaintiffs failed to cure the same or similar deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 14-16. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs' CCCL claims were deficient for the same or similar reasons as stated in this Order. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CCCL claims with prejudice.

E. Claim for Unjust Enrichment

Plaintiffs' fifth and final claim is for unjust enrichment. SAC ¶¶ 129-33. However, California does not recognize a separate cause of action for unjust enrichment. *See Hill v. Roll*

Int'l Corp., 195 Cal. App. 4th 1295, 1307 (2011) ("Unjust enrichment is not a cause of action, just a restitution claim."). As a result, courts have consistently dismissed stand-alone claims for unjust enrichment. *See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012); *Robinson v. HSBC Bank USA*, 732 F. Supp. 2d 976, 987 (N.D. Cal. 2010).

In some circumstances, courts have construed purported claims for unjust enrichment as quasi-contract claims seeking restitution. *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015); *see also Swafford v. Int'l Bus. Mach. Corp.*, 383 F. Supp. 3d 916, 931-32 (N.D. Cal. 2019) (construing unjust enrichment cause of action as a quasi-contract claim). A quasi-contract cause of action seeks "to prevent unjust enrichment in the absence of a true contract or where the contract was obtained by fraud." *Fowler v. Wells Fargo Bank, N.A.*, 2017 WL 3977385, at *5 (N.D. Cal. Sept. 11, 2017) (citing *McBride v. Boughton*, 123 Cal. App. 4th 379, 388 (2004)). However, "an action based on an implied-in-fact or quasi-contract cannot lie where there exists between the parties a valid express contract covering the same subject matter." *Tsai v. Wang*, 2017 WL 2587929, at *7 (N.D. Cal. June 14, 2017) (quoting *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014)); *see also Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1388 (2012) ("A plaintiff may not . . . pursue or recover on a quasi-contract if the parties have an enforceable agreement regarding a particular subject matter.").

Plaintiffs now contend that they adequately plead a quasi-contract claim seeking restitution for unjust enrichment. Opp. at 15. They are mistaken. Courts have repeatedly held that "a plaintiff may not plead the existence of an enforceable contract and simultaneously maintain a quasi-contract claim unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid." *Tsai*, 2017 WL 2587929, at *7; *Adtrader, Inc. v. Google LLC*, 2018 WL 3428525, at * 11 (N.D. Cal. July 13, 2018) ("[T]o assert such a claim [for unjust enrichment], Plaintiffs must allege that the parties do not have an enforceable contract pertaining to Google's advertisement services."); *Deras v. Volkswagen Grp. of Am., Inc.*, 2018 WL 2267448, at *3 (N.D. Cal. May 17, 2018) ("[A] quasi-contract action for unjust enrichment does not lie where express binding agreements exist and define the parties' rights." (quoting *Gerstle v. Am. Honda Motor*

Co., 2017 WL 2797810, at *14 (N.D. Cal. June 28, 2017))).

Here, the SAC alleges that "Plaintiffs have a contract with Apple pursuant to the Terms of Use of Apple Devices and Services that is breached by Apple's interference as alleged," SAC ¶ 131, but the SAC does not plead any allegations suggesting that this contract is unenforceable or invalid. Plaintiffs, however, contend that they are entitled to plead alternative or inconsistent theories of recovery under Federal Rule of Civil Procedure 8(d)(2). Opp. at 15.

To be sure, Rule 8 allows a party to set out two or more claims hypothetically and regardless of consistency. Fed. R. Civ. P. 8(e)(2)-(3). However, "[e]ven though [Rule 8] of the Federal Rules of Civil Procedure allows a party to state multiple, even inconsistent claims, it does not alter a substantive right between the parties and accordingly does not allow a plaintiff invoking state law to an unjust enrichment claim while also alleging an express contract." *Deras*, 2018 WL 2267448, at *3 (quoting *Gerlinger v. Amazon.com, Inc.*, 311 F. Supp. 2d 838, 856 (N.D. Cal. 2004)). Indeed, "[a] plaintiff may assert inconsistent theories of recovery at the pleading stage, including inconsistent claims alleging both the existence and the absence of an enforceable contract. However, a plaintiff may not plead the existence of an enforceable contract and simultaneously maintain a quasi-contract claim unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid." *Tsai*, 2017 WL 2587929, at *7 (citations omitted). As a result, because Plaintiffs fail to allege that their contract with Apple is unenforceable or invalid, the SAC fails to state a quasi-contract claim for unjust enrichment.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' unjust enrichment claim. Plaintiffs failed to cure similar deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 16-17. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs' unjust enrichment claim was deficient for similar reasons as stated in this Order. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' unjust enrichment claim with prejudice.

F. Rule 8 and Statutes of Limitations

Finally, the Court addresses Apple's Rule 8 and statute of limitations argument. Apple notes that "[n]otwithstanding the opportunity to amend their Complaint, the SAC is silent as to when the Plaintiffs [Bishop, Schwartz, Richardson, and Kyslowsky] first enabled 2FA." Mot. at 8, n.4. Additionally, Apple contends that Plaintiff Brodsky's CIPA, CFAA, and CCCL claims are time-barred and that Plaintiff Tracey's CIPA claim is time-barred. Mot. at 8-9.

Plaintiff Brodsky alleges that he enabled 2FA on his Apple devices in September 2015. SAC ¶ 37. Plaintiff Tracey now alleges that he enabled 2FA on his Apple devices in September 2017. *Id.* ¶ 38. Plaintiff Brodsky did not file the instant putative class action until February 8, 2019, approximately three and a half years after Plaintiff Brodsky alleges that he enabled 2FA on his Apple devices and more than sixteen months after Plaintiff Tracey alleges that he enabled 2FA on his Apple devices. ECF No. 1. As before, the remaining Named Plaintiffs—Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky—do not allege when 2FA was enabled on their devices. SAC ¶ 39; *see* Order at 17 ("However, in line with the overall vagueness of Plaintiffs' FAC, [some Named] Plaintiffs . . . do not allege when 2FA was enabled on their Apple devices.").

The longest applicable statute of limitations is three years. Under the CIPA, the applicable statute of limitations is one year. *Ion Equip. Corp. v. Nelson*, 110 Cal. App. 3d 868, 880 (1980) ("The statute of limitations in which to commence an action for invasion of privacy is one year."). Under the CFAA, the statute of limitations is two years from "the date of the act complained of or the date of the discovery of the damage." 18 U.S.C. § 1030(g). Under the CCCL, the statute of limitations is three years. Cal. Penal Code § 502(e)(5). The Court first addresses Rule 8's pleading standard as to Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky before turning to the statutes of limitations argument as to Plaintiffs Brodsky and Tracey.

1. Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky Fail to Satisfy Rule 8 For Their CIPA, CFAA, and CCCL Claims

At the outset, the Court acknowledges that Apple has the burden of proof to support its statute of limitations defenses as to Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky. Opp. at 5. However, the issue with the SAC with regard to Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky is not a statute of limitations problem, but rather, a Rule 8 problem.

Courts often dismiss claims under Rule 8 when plaintiffs fail to allege approximately when the actionable misconduct occurred. *See Mir v. City of Torrance*, 2018 WL 6133712, at *1 (C.D. Cal. Oct. 17, 2018) ("Although twice directed to do so by the Court, Plaintiff has not attributed most of the alleged acts to any Defendant nor alleged when most of them occurred, leaving the Court and Defendants to attempt to parse out who is accused of doing what and when. This is improper." (citations omitted)); *Vasconcellos v. Sara Lee Bakery*, 2013 WL 4014520, at *2 (N.D. Cal. Aug. 5, 2013) (concluding plaintiffs' claims were "insufficiently pled" in part because "[t]he complaint d[id] not allege when plaintiff worked for defendants, when plaintiff became injured or engaged in protected activity, or when the alleged misconduct occurred"); *O'Donnell v. U.S. Bancorp Equip. Fin., Inc.*, 2010 WL 2198203, at *3 (N.D. Cal. May 28, 2010) ("However, the Court finds that O'Donnell has nonetheless failed to satisfy the pleading requirements of Federal Rule of Civil Procedure 8 because she has not alleged any dates in her complaint. *See, e.g., Swierkiewicz*, 534 U.S. at 514 (finding complaint to be sufficient in part because it "provided relevant dates"). Without any reference to when the alleged misconduct occurred, O'Donnell's allegations fail to state a plausible claim for relief.").

This is especially true here because Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky do not allege when 2FA was enabled on their devices, and Apple has raised the non-frivolous possibility of multiple statute of limitations defenses. The Court notes that a failure to plead when any alleged misconduct occurred will not necessarily be fatal under Rule 8. However, where, as here, an applicable statute of limitations defense has been raised and is non-frivolous, Plaintiffs' repeated failure to plead the approximate date of alleged misconduct fails to satisfy Rule 8's requirement to "contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th

Cir. 2011); *see also Calip v. M.E.I.C.*, 2015 WL 5996365, at *6 (N.D. Cal. Oct. 15, 2015) ("Nor does Plaintiff state when she was in the hospital and when her child passed away, without which the Court cannot determine whether Plaintiff brought her claims within the applicable statute of limitations period."). Indeed, the Court previously cautioned Plaintiffs that the FAC was vague as to multiple Plaintiffs' allegations regarding when 2FA was enabled on their Apple devices. Order at 17. Nonetheless, Plaintiffs largely failed to cure those same defects in the SAC.

As a result, because the SAC does not plead when 2FA was enabled for Plaintiffs Bishop, Schwartz, Richardson, and Kyslowsky and therefore fails to satisfy Rule 8's pleading standard, the Court dismisses Plaintiffs Bishop's, Schwartz's, Richardson's, and Kyslowsky's CIPA, CFAA, and CCCL claims. These Plaintiffs failed to cure similar deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 17-20. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that Plaintiffs Bishop's, Schwartz's, Richardson's, and Kyslowsky's CIPA, CFAA, and CCCL claims were deficient for similar reasons as stated in this Order. Accordingly, the Court dismisses these claims with prejudice.

2. The Statute of Limitations Bars Plaintiff Brodsky's CIPA, CFAA, and CCCL Claims and Plaintiff Tracey's CIPA Claim

As noted previously, the CIPA's statute of limitations is one year, the CFAA's statute of limitations is two years, and the CCCL's statute of limitations is three years. Therefore, because Plaintiff Brodsky enabled 2FA in September 2015, the statute of limitations ran for Plaintiff Brodsky's CIPA claim in September 2016, his CFAA claims in September 2017, and his CCCL claims in September 2018. Thus, Plaintiff Brodsky's CIPA, CFAA, and CCCL claims are time-barred. Similarly, because Plaintiff Tracey enabled 2FA in September 2017, the statute of limitations ran for Plaintiff Tracey's CIPA claim in September 2018 such that Plaintiff Tracey's CIPA claim is also time-barred.

Acknowledging this, Plaintiffs contend that Plaintiff Brodsky's CIPA, CFAA, and CCCL claims and Plaintiff Tracey's CIPA claim are nonetheless timely pursuant to the continuous accrual doctrine, the continuing violation doctrine, and the delayed discovery rule. Opp. at 4-5. However, none of these doctrines apply to toll the relevant statutes of limitations.

a. The Continuous Accrual Doctrine Does Not Apply

Under California law, the continuous accrual doctrine recognizes that "a series of wrongs or injuries may be viewed as each triggering its own limitations period, such that a suit for relief may be partially time-barred as to older events . . . but timely as to those within the applicable limitations period." *Wolf v. Travolta*, 167 F. Supp. 3d 1077, 1104 (C.D. Cal. 2016) (quoting *Aryeh v. Canon Bus. Solutions, Inc.*, 55 Cal. 4th 1185, 1192 (2013)). "Generally speaking, continuous accrual applies whenever there is a continuing or recurring obligation: When an obligation or liability arises on a recurring basis, a cause of action accrues each time a wrongful act occurs, triggering a new limitations period." *Aryeh*, 55 Cal. 4th at 1199 (quotation marks omitted). In *Aryeh v. Canon Business Solutions, Inc.*, the question before the California Supreme Court was "when a UCL claim accrues." *Id*. at 1192. The California Supreme Court found that the continuous accrual doctrine can apply to UCL claims when the claims involved unlawful charges in monthly bills, but also explained that "[t]o determine whether the continuous accrual doctrine applies here," courts "look not to the claim's label as a UCL claim but to the nature of the obligation allegedly breached." *Aryeh*, 55 Cal. 4th at 1200.

California courts have largely confined the application of the continuing accrual theory to "a limited category of cases, including installment contracts, leases with periodic rental payments, and other types of periodic contracts that involve no fixed or total payment amount." *Lamont v. Time Warner, Inc.*, 2012 WL 6146681, at *5 (C.D. Cal. Dec. 11, 2012). This court has repeatedly noted that when an alleged duty "bears little relation to the monthly payments or monthly bills that California courts have found to be periodic, recurring obligations," applying the continuous accrual doctrine is unwarranted. *See Garrison v. Oracle Corp.*, 159 F. Supp. 3d 1044, 1083-84 (N.D. Cal. 2016); *see also State ex rel. Metz v. CCC Info. Servs., Inc.*, 149 Cal. App. 4th 402, 418 (2007) (holding that the continuous accrual doctrine does not apply where "[the plaintiff's] action does not involve a recurring obligation or any such period payment obligations"); *Tsemetzin v. Coast Fed'l Sav. & Loan Ass'n*, 57 Cal. App. 4th 1334, 1344 (1997) (applying the continuous accrual doctrine to a dispute over monthly rent payments); *Armstrong Petroleum Corp. v. Tri-Valley Oil & Gas Co.*, 116 Cal. App. 4th 1375, 1388-89 (2004) (applying the continuous accrual doctrine to a dispute over monthly lease payments). Indeed, a "continuing obligation to avoid anticompetitive behavior is not a periodic, recurring obligation such as a monthly payment or monthly bill, and as such, the continuous accrual doctrine does not apply." *Ryan v. Microsoft Corp.*, 147 F. Supp. 3d 868, 896 (N.D. Cal. 2015).

Here, Plaintiffs attempt to conform the SAC to the Court's prior Order by alleging that Plaintiffs made periodic payments for Apple Services and third-party apps. Plaintiffs, however, do not argue that Apple breached a continuing duty by unlawfully charging them for payments for their Apple Services or third-party apps. Order at 18 ("The continuous accrual doctrine applies where the defendant owes the plaintiff a continuing duty 'susceptible to recurring breaches.'" (quoting *Aryeh*, 55 Cal. 4th at 1200)). Rather, the gravamen of the SAC is that Apple unlawfully upgraded Plaintiffs' Apple devices to 2FA, which occurs at a discrete point in time. SAC ¶¶ 1-4, 37-38. Therefore, the SAC's description of the alleged duty that Apple owed and breached is best characterized as an obligation not to unlawfully force Plaintiffs to use 2FA. But just as this Court previously concluded that a "continuing obligation to avoid anticompetitive behavior is not a periodic, recurring obligation such as a monthly payment or monthly bill," Apple's "continuing obligation" to avoid forcing Plaintiffs to use 2FA is also not a periodic, recurring obligation. *See Ryan*, 147 F. Supp. 3d at 896; *see also Factory Direct Wholesale, LLC v. iTouchless Housewares & Prod., Inc.*, 411 F. Supp. 3d 905, 918 (N.D. Cal. 2019) ("Defendant's continuing obligation to avoid illegal behavior that violates the UCL is also not a periodic, recurring obligation."). "[A]s such, the continuous accrual doctrine does not apply." *Ryan*, 147 F. Supp. 3d at 896.

United States District Court
Northern District of California

b. The Continuing Violation Doctrine Does Not Apply

Plaintiffs next argue that the continuing violation doctrine applies and thus tolls the relevant statutes of limitations. Unlike the continuous accrual doctrine, the continuing violation doctrine "renders an entire course of conduct actionable," including wrongful acts that would otherwise be untimely. *Aryeh*, 5 Cal. 4th at 1199. The continuing violation doctrine applies when "a wrongful course of conduct [becomes] apparent only through the accumulation of a series of harms" but not when a plaintiff experiences "a series of discrete, independently actionable alleged wrongs." *Id.* at 1198. The complaint must feature "[a]llegations of a pattern of reasonably frequent and similar acts." *Id.*

The Court previously concluded that the continuing violation doctrine did not save Plaintiffs' claims because "the continuing violation doctrine applies only where 'a wrongful course of conduct [becomes] *apparent* only through the accumulation of a series of harms.'" Order at 19 (quoting *Aryeh*, 55 Cal. 4th at 1198). Because "[a]ny user allegedly injured by 2FA would doubtless be aware of that injury on the user's first attempt to log in to his Apple ID via 2FA," "the continuing violation doctrine does not apply." *Id*.

That same conclusion applies again here. The SAC alleges that "2FA increases the complexity of using the Apple devices, Services[,] and Third-Party Apps for Plaintiffs and Class, especially for Senior Plaintiffs and Senior Class Members," SAC ¶ 41, but that allegation does not indicate that users would not "be aware of their injury on the user's first attempt to log in to [their] Apple ID via 2FA," Order at 19. In fact, the SAC's allegations include figures that prominently display 2FA covering a device's entire screen, and the SAC alleges that 2FA delays Plaintiffs' ability to log in to Apple ID or their Apple devices as soon as 2FA is enabled. SAC ¶¶ 35-36, 38-41. In short, none of the SAC's allegations alter the Court's previous conclusion that "[a]ny user allegedly injured by 2FA would doubtless be aware of that injury on the user's first attempt to log in to his Apple ID via 2FA." Order at 19. Thus, the alleged wrongful course of conduct does not become apparent only through the accumulation of a series of harms as required by the continuing violation doctrine. Accordingly, the continuing violation doctrine does not apply to rescue the time-barred claims.

c. The Delayed Discovery Rule Does Not Apply

Finally, as before, Plaintiffs cannot rely on the delayed discovery rule. Under the delayed discovery rule, "the accrual of the action may be postponed and the running of the limitations period tolled until the plaintiff discovers, or has reason to discover the cause of action." *Quarry v. Doe I*, 53 Cal. 4th 945, 960 (2012) (citation omitted). "A plaintiff has reason to discover a cause of action when he or she has reason to at least suspect a factual basis for its elements." *Id.* Plaintiffs' SAC includes no allegations of delayed discovery, and Plaintiff's opposition brief recycles the exact same arguments from Plaintiffs' prior opposition brief that the Court previously rejected. *Compare* Opp. at 5, *with* ECF No. 34 at 6. Plaintiffs' SAC alleges that 2FA delays Plaintiffs' ability to log in to Apple ID or their Apple devices as soon as 2FA is enabled. SAC ¶¶ 35, 38-39. Therefore, any user allegedly injured by 2FA would be aware of that injury on the user's first attempt to log in via 2FA. As a result, the delayed discovery rule does not apply.

Accordingly, the statute of limitations bars Plaintiff Brodsky's CIPA, CFAA, and CCCL claims and Plaintiff Tracey's CIPA claim. Therefore, the Court GRANTS Apple's motion to dismiss Plaintiff Brodsky's CIPA, CFAA, and CCCL claims and Plaintiff Tracey's CIPA claim on that ground. Plaintiffs failed to cure the same deficiencies the Court previously identified in its prior Order, and the SAC offers no new facts to justify a different conclusion. Order at 17-19. As the Court previously warned, "failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice." *Id.* at 20. Furthermore, courts are justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *Carvalho*, 629 F.3d at 892. This is precisely the situation here, as the Court's prior Order put Plaintiffs on notice that many of their claims were time-barred. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiff Brodsky's CIPA, CFAA, and CCCL claims and Plaintiff Tracey's CIPA claim with prejudice.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS Apple's motion to dismiss with prejudice.

IT IS SO ORDERED.

Dated: April 7, 2020

Lucy H. Koh

LUCY H. KOH
United States District Judge