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 WITHOUT PREJUDICE APPLE'S MOTION TO DISMISS** Re: Dkt. No. 32

Plaintiffs Jay Brodsky, Brian Tracey, Alex Bishop, and Brendan Schwartz ("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. Before the Court is Apple's motion to dismiss Plaintiffs' first amended complaint ("FAC"). Having considered the submissions of the parties, the relevant law, and the record in this case, the Court GRANTS Apple's motion to dismiss without prejudice.

I. BACKGROUND

A. Factual Background

Plaintiffs are individuals residing in the United States. ECF No. 13 ("FAC"), ¶ 7. Apple is a California corporation that designs and sells products including iPhones, iPads, Macbooks, Apple TVs, and Apple Watches. *Id.* ¶¶ 8, 14. Once a consumer buys an Apple product, the Apple product is associated with the consumer's Apple ID, which is the individual's email address. *Id.* An Apple ID is required to use Apple services, such as FaceTime and iMessage. *Id.* ¶ 15.

Plaintiffs allege that Apple's provision of two-factor authentication ("2FA") as an Apple ID login process violates Plaintiffs' right to privacy. *Id.* ¶ 1. 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.* ¶ 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. *Id.* 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.*

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 Apple ID security questions will expire on October 15, 2018." *Id.* ¶ 18. Plaintiffs allege that the link allowing a user to disable 2FA expires within 14 days after 2FA's enablement. *Id.* 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.*

Plaintiff Brodsky alleges that in September 2015, a software update enabled 2FA for Plaintiff Brodsky's Apple ID. *Id.* ¶ 19.

Plaintiff Tracey alleges that he was "forced to enable 2FA for a software update on his Apple devices." *Id.* ¶ 20.

Plaintiff Bishop alleges that "based on an unforeseen consequence outside of his control," he lost access to his second trusted Apple device, which he used for 2FA. *Id.* ¶ 21. Plaintiff Bishop could not access Apple services using Apple ID "for days." *Id.*

Plaintiff Schwartz alleges that he lost his second trusted Apple device "based on events outside of his control." *Id.* ¶ 22. Then, Apple placed Plaintiff Schwartz in its account recovery process and Plaintiff Schwartz could not use his Apple ID "for months." *Id.*

B. Procedural History

On February 8, 2019, Plaintiff Brodsky filed this lawsuit against Apple. ECF No. 1. On March 29, 2019, Plaintiffs filed the FAC, with Tracey, Bishop, and Schwartz added as named Plaintiffs. ECF No. 13. The FAC alleges five causes of action: (1) trespass to chattels, *id.* ¶¶ 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 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. ¶ 29. The class period began "when Apple introduced 2FA in 2015." *Id.* ¶ 28.

On May 1, 2019, Apple filed the instant motion to dismiss Plaintiffs' FAC. ECF No. 32 ("Mot."). On May 15, 2019, Plaintiffs filed an opposition. ECF No. 34 ("Opp."). On May 22, 2019, Apple filed a reply in support of its motion to dismiss. ECF No. 37 ("Reply").

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 continued the May 22, 2019 case management conference to September 25, 2019 and stayed discovery "until the Court orders otherwise." ECF No. 36.

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 accept as true allegations contradicted by judicially noticeable facts, *see Schwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it "may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the Court "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). 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. Rule 15(a) of the Federal Rules of Civil Procedure states that 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. Thus, 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).

III. DISCUSSION

Apple moves to dismiss each of Plaintiffs' claims for failure to state a claim. Apple also contends that certain claims are barred by the statute of limitations or must be dismissed because Plaintiffs fail to allege their states of residence. The Court first addresses the sufficiency of each of Plaintiffs' individual claims. Then, the Court addresses Apple's other arguments that the FAC is deficient.

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." FAC ¶ 48.

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)).

Apple argues that: (1) Apple did not enable 2FA without Plaintiffs' authorization; and (2)

United States District Court
Northern District of California

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. Accordingly, in the context of a software update, "[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).

In the instant case, Plaintiffs do not allege facts to indicate that Plaintiffs failed to authorize the enablement of 2FA. Rather, Plaintiffs' FAC alleges that 2FA is enabled when an Apple ID user voluntarily turns on 2FA, installs a software update, or creates a new Apple ID. FAC ¶ 16. None of those means to enable 2FA permits Apple to enable 2FA unilaterally and without Plaintiffs' authorization.

In conclusory fashion, Plaintiff Brodsky alleges that his devices "had a software update that enabled 2FA for Apple ID without his knowledge or consent on or around September of 2015," and Plaintiff Tracey alleges that 2FA was "forced" upon him through a software update. FAC ¶¶ 19–20. Plaintiffs concede in their opposition that Plaintiffs voluntarily installed the software update, but contend that Plaintiffs did not specifically authorize the enablement of 2FA. *See* Opp. at 8. 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.*, 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.* Thus, the plaintiffs did not consent to those additional effects of the software update.

By contrast, Plaintiff Brodsky has offered no information about the 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. Nor has Plaintiff Tracey alleged any facts related to his "forced" enablement of 2FA. Plaintiffs' bald assertions in the FAC that they did not consent to enablement of 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"). Although Plaintiffs raise such arguments in their opposition brief, these allegations do not appear in the FAC, and Plaintiffs have not alleged that any interference with their devices was not authorized by Plaintiffs. In fact, neither Plaintiff Bishop nor Plaintiff Schwartz even specifies how they enabled 2FA on their Apple devices, or alleges that enablement was involuntary. *See* FAC ¶¶ 21–22.

2. Plaintiffs Have Not Alleged that Any Trespass Harmed Plaintiffs

Plaintiffs have also 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).

In the instant case, Plaintiffs allege that "[e]ach login process takes an additional estimated 2-5 more minutes with 2FA." FAC ¶ 17. Plaintiffs' allegations are plainly 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, a delay of 2-5 minutes does not impair the functioning of Plaintiffs' Apple devices or Apple IDs. 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). Plaintiffs' opposition argues that Plaintiffs suffer "dispossession" and are "blocked 100% from accessing their own devices," in an apparent attempt to parrot the language of *Hamidi*. Opp. at 12. However, Plaintiffs do not identify any such allegation in the FAC, nor do Plaintiffs explain whether the alleged "100%" blockage is distinct from the 2-5 minute login delay.

Alternatively, Plaintiffs contend that Plaintiffs suffer longer dispossessions "when access to a trusted device to receive 2FA passcode [sic] is lost." Opp. at 10. However, Plaintiffs do not allege that Apple or 2FA led Plaintiffs to lose access to their trusted devices. 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." FAC ¶¶ 21–22. In neither instance 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 that Apple interfered with Plaintiffs' possession of their devices.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' trespass to chattels claim. Because granting Plaintiffs an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiffs have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

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

Next, the Court discusses 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." FAC ¶ 54.

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). The CIPA 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, even though the face of Plaintiffs' own pleading indicates that "[t]wo-factor authentication 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." FAC ¶ 18.

In its motion to dismiss, Apple principally argues 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 Fail 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").

In the instant case, Plaintiffs allege only that Apple intercepted "Plaintiffs' login activities through 2FA that requires connecting with Apple's servers on the internet." FAC ¶ 26. Thus, the only communications that Plaintiffs allege 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.

Ramos v. Capitol One, N.A., 2017 WL 3232488 (N.D. Cal. July 27, 2017), is not to the contrary. 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. *Id.* at *9. *Ramos* is inapplicable to the instant case, in which Plaintiffs' "login activities" are communications that Plaintiffs send to Apple's servers. Unlike in *Ramos*, Plaintiffs do not allege that Apple is intercepting via its servers Plaintiffs' communications with a third party. Moreover, other Apple ID login methods presumably also require Plaintiffs to communicate with Apple's servers. Yet Plaintiffs do not challenge those login methods as invasions of privacy. Thus, Plaintiffs have failed to allege that via 2FA, Apple was a third party that intercepted Plaintiffs' communications with another entity.

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). For example, 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 only that Apple intercepted Plaintiffs' "login activities," or presumably Plaintiffs' user names and passwords. *In re Zynga* forecloses a CIPA claim predicated on such record information. *In re Carrier IQ* explicitly held that user names and passwords are not "contents" under the Wiretap Act. 78 F. Supp. 3d at 1082, 1084. Plaintiffs attempt to distinguish these precedents by contending 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. See Opp. at 14. 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." Thus, Plaintiffs have failed to allege the contents of any communication that Apple intercepted.

Moreover, the only communications discussed in Plaintiff's FAC are Plaintiff's communications with Apple, which are not third-party communications. Because Plaintiffs' communications with Apple are not communications with a third party, Apple cannot "intercept" them.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CIPA claim. Because granting Plaintiffs an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiffs have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

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." FAC ¶¶ 71–72. 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.* at § 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). Under the CFAA, Plaintiffs must also plead that Apple's actions caused 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 is exceedingly skeptical of Plaintiffs' theory that 2FA—an Apple login method that according to Plaintiff's 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. FAC ¶ 18.

In its motion to dismiss, Apple contends 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 agrees.

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." Accordingly, the Ninth Circuit has held that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016). For example, in *Power Ventures*, the defendant had "arguable permission to access Facebook's computers" until Facebook expressly rescinded that authorization via a cease and desist letter. *Id.*

As explained in the discussion of Plaintiffs' trespass to chattels claim, Plaintiffs only conclusorily allege that Plaintiffs did not authorize 2FA, but concede that Plaintiffs voluntarily installed the software update that enabled 2FA. On that ground alone, Plaintiffs' CFAA claim fails. In the CFAA context, a user would have "serious difficulty" pleading a CFAA violation based on the voluntary installation of software. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066 (N.D. Cal. 2012); *see also In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 452 (N.D. Cal. 2018) (holding that plaintiffs authorized Apple's access to devices when they "chose to voluntarily download and install" Apple's software updates); *In re Sony PS3 Other OS Litig.*, 551 F. App'x 916, 923 (9th Cir. 2014) (holding that voluntary installation rebuts a claim of unauthorized access under the CFAA). As explained above, Plaintiffs Brodsky and Tracey enabled 2FA when they downloaded software updates from Apple. *Id.* ¶¶ 19–20.

To the extent Plaintiffs attempt to allege that Apple exceeded Plaintiffs' authorization, Plaintiffs do not allege that Plaintiffs revoked any consent for Apple's servers to receive Plaintiffs' login activities. 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. Moreover, Plaintiffs do not allege any facts related to the scope of Plaintiff Brodsky's authorization when he downloaded the software update, such as that Plaintiff Brodsky authorized Apple to access his Apple ID and device for all purposes except for 2FA, or that Apple hid information about 2FA in the message that accompanied the software update. *See Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1070 (N.D. Cal. 2018) (holding that allegations of "hidden" software were sufficient to allege that the defendant's access exceeded the plaintiff's authorization).

Plaintiffs' legal conclusion that Apple's access to Plaintiffs' Apple IDs was unauthorized is insufficient to state a claim. This is particularly true given the Ninth Circuit's instruction that the CFAA was enacted "primarily to address the growing problem of computer hacking," and that the CFAA should be interpreted narrowly. *Nosal*, 676 F.3d at 858. The facts alleged in the FAC permit no inference that Apple "hacked" into Plaintiffs' devices or Apple IDs. Allowing CFAA claims to proceed on such conclusory, thin allegations "would expand the CFAA too far." *In re*

Apple Inc. Device Performance Litig., 347 F. Supp. 3d at 453. At base, Plaintiffs' FAC alleges a claim that 2FA slows down the login process, not a hacking claim.

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

Second, Plaintiffs have failed to plead damages under the CFAA. Although Plaintiffs make the conclusory allegation that Plaintiffs suffered "economic loss with an aggregated value of at least $5,000 during a one-year period," Plaintiffs allege no facts to support that conclusion. FAC ¶ 76. At most, Plaintiffs allege that 2FA delays Plaintiffs' login to their Apple IDs by 2-5 minutes. *Id.* ¶ 17. Even the allegation that an application "consume[s] valuable memory space" is insufficient to allege that the application "impairs Plaintiffs' devices or interrupts service" sufficient to show $5,000 in damage under the loss requirements of the CFAA. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067. Plaintiffs do not allege the dollar value of any alleged damages in the FAC, let alone dollar values that could amount to $5,000. In sum, Plaintiffs' bald assertion of $5,000 in damages based on 2-5 minute login delays without any facts to support the allegation is "insufficient to sustain a CFAA claim." *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 949 (N.D. Cal. 2014).

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' CFAA claim. Because granting Plaintiffs an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiffs have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

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. *Facebook, Inc. v. Grunin*, 77 F. Supp. 3d 965, 971 (N.D. Cal. 2015).

Plaintiffs bring claims under five provisions of the CCCL, Cal. Penal Code §§ 502(c)(1), (3-5), (7). For each claim, Plaintiff alleges that Apple "knowingly and without permission" accessed, altered, or otherwise disrupted Plaintiffs' Apple devices. FAC ¶¶ 60–64. 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." To allege that a defendant acted without permission under the CCCL, a plaintiff must allege that 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. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1101 (N.D. Cal. 2015); *see also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014) (explaining that parties act without permission when they "circumvent[] technical or code-based barriers") (alteration in original) (citation omitted). In the instant case, Plaintiffs offer no allegations about how Plaintiffs attempted to prevent 2FA's access to their information, or how 2FA offers Apple access to Plaintiffs' information that is somehow different from Apple's access through other Apple ID login methods.

Again, Plaintiffs make only the conclusory allegation that Plaintiff Brodsky's voluntary installation of the software update did not equate to voluntary installation of 2FA. However, Plaintiff Brodsky has offered no information about the 2015 software update that allegedly enabled 2FA on his phone, nor about whether Plaintiff Brodsky read or reviewed the message that accompanied the software update and whether that message disclosed that the update would enable 2FA. Plaintiff Brodsky's bald assertion that he did not give Apple permission to enable 2FA is a legal conclusion not entitled to the presumption of truth. *See In re Gilead*, 536 F.3d at 1055 (holding that a court need not accept as true "allegations that are merely conclusory").

Moreover, Plaintiffs' specific CCCL claims all merely parrot the language of the CCCL. For example, 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." 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." The FAC includes no factual allegations about (1) how, through 2FA, Apple was able to "use" Apple Services and third-party apps; (2) which Apple Services or third-party apps Apple allegedly "caused to be used"; or (3) 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 claim. Because granting Plaintiffs an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiffs have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

E. Claim for Unjust Enrichment

Plaintiffs' fifth claim is for unjust enrichment. FAC ¶ 79. However, as Apple points out, 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). Generally, courts have approved quasi-contract claims premised on false and misleading labels. *See Khasin v. R.C. Bigelow, Inc.*, 2015 WL 4104868, at *3 (N.D. Cal. July 7, 2015) (citing cases).

In the instant case, Plaintiffs' FAC includes no allegation that Apple is liable in quasi-contract or that 2FA was somehow mislabeled. In their unjust enrichment claim, Plaintiffs conclusorily allege that Apple has retained "information regarding online communications and activities of Plaintiffs and the Class." FAC ¶ 80. Plaintiffs' unjust enrichment claim thus appears pled as a stand-alone cause of action, and dismissal is warranted.

Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' unjust enrichment claim. Because granting Plaintiffs an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiffs have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

Finally, the Court addresses Apple's two other arguments about deficiencies in Plaintiffs' FAC.

F. The Statute of Limitations Bars Plaintiff Brodsky and the Putative Class's Claims Under the CIPA, CCCL, and CFAA

First, Apple contends that Plaintiff Brodsky's and the putative class's claims under the CIPA, CCCL, and CFAA are all time-barred by the applicable statute of limitations.

Plaintiff Brodsky alleges that he enabled 2FA on his Apple devices in September 2015. FAC ¶ 19. Similarly, Plaintiffs' class period began "when Apple introduced 2FA in 2015." *Id.* ¶ 28. 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 three years after Plaintiff's class period began. ECF No. 1. However, in line with the overall vagueness of Plaintiffs' FAC, Plaintiffs Tracey, Bishop, and Schwartz do not allege when 2FA was enabled on their Apple devices. *See* FAC ¶¶ 20–22.

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). Accordingly, because Plaintiff Brodsky and the putative class enabled 2FA in 2015, the statute of limitations ran for their CIPA claims in 2016, their CFAA claims in 2017, and their CCCL claims in 2018. Thus, Plaintiff Brodsky and the putative class's CIPA, CCCL, and CFAA claims are time-barred.

Acknowledging this, Plaintiffs contend that Plaintiff Brodsky and the putative class's CIPA, CCCL, and CFAA claims are timely under the continuous accrual and continuing violation doctrines. Opp. at 4. However, neither doctrine applies.

Under the continuous accrual doctrine, "a series of wrongs or injuries may be viewed as each triggering its own limitations period, such as that a suit for relief may be partially time-barred as to older events but timely as to those within the applicable limitations period." *Aryeh v. Canon Bus. Sols., Inc.*, 55 Cal. 4th 1185, 1198 (2013). The continuous accrual doctrine applies where the defendant owes the plaintiff a continuing duty "susceptible to recurring breaches." *Id.* at 1200. For example, in *Aryeh*, the defendant allegedly imposed unfair monthly charges on the plaintiff. *Id.* Generally, courts have applied the continuous accrual theory only to instances in which a plaintiff has "asserted a right to, or challenged the assessment of, periodic payments." *Baxter v. State Teachers Retirement Sys.*, 18 Cal. App. 5th 340, 378 (2017); *see also Garrison v. Oracle Corp.*, 159 F. Supp. 3d 1044, 1083 (N.D. Cal. 2016) (finding the continuous accrual doctrine inapplicable where the plaintiff did not allege any right to periodic payments).

In the instant case, Plaintiffs have not alleged any right to periodic payments, or challenged Apple's assessment of a periodic obligations. Accordingly, the continuous accrual doctrine does not apply.

Unlike continuous accrual, 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 theory 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.*

Plaintiffs contend that the FAC alleges a pattern of frequent and similar acts because after 2FA is enabled, Plaintiffs must use 2FA for each login and are thus injured on an ongoing basis. Opp. at 5. To the contrary, the FAC alleges that Plaintiffs can disable 2FA within 14 days of enablement, which contradicts Plaintiffs' argument. However, even if Plaintiffs' argument is true, the continuing violation doctrine applies only where "a wrongful course of conduct [becomes] *apparent* only through the accumulation of a series of harms." *Aryeh*, 55 Cal. 4th at 1198. Any 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. Accordingly, the continuing violation doctrine does not apply.

For similar reasons, Plaintiffs also cannot rely on the delayed discovery rule. Under the 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' FAC includes no allegations of delayed discovery. Rather, Plaintiffs allege that 2FA delays Plaintiffs' ability to log in to Apple ID or their Apple devices as soon as 2FA is enabled. FAC ¶ 16. Accordingly, any user allegedly injured by 2FA would be aware of that injury on the user's first attempt to log in via 2FA.

Therefore, the statute of limitations bars Plaintiff Brodsky's and the putative class's claims under the CIPA, CCCL, and CFAA, and the Court GRANTS Apple's motion to dismiss Plaintiff Brodsky and the putative class's CIPA, CCCL, and CFAA claims on that ground. Because granting Plaintiff Brodsky and the putative class an additional opportunity to amend the complaint would not be futile, cause undue delay, or unduly prejudice Apple, and Plaintiff Brodsky and the putative class have not acted in bad faith, the Court grants leave to amend. *See Leadsinger, Inc.*, 512 F.3d at 532.

G. Standing for Common Law Claims

Finally, Apple also contends that Plaintiffs lack standing to bring their common law claims for trespass to chattels and unjust enrichment because Plaintiffs fail to allege their states of residence. *See* FAC ¶ 7 (alleging only that Plaintiffs are "individuals residing in the United States"). However, the cases that Apple cites do not stand for the precise proposition that a court may dismiss common law claims for lack of standing when a plaintiff fails to allege his state of residence. Rather, in *Johnson*, for example, the court assessed whether named plaintiffs resident in two states could bring claims under other states' common laws. *Johnson v. Nissan N. Am., Inc.*, 272 F. Supp. 3d 1168, 1175 (N.D. Cal. 2017).

In the instant case, Plaintiffs have not even alleged their states of residence. Plaintiffs' FAC thus does not present a *Johnson* problem, but rather a failure under Rule 8 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). Without any notice as to Plaintiffs' states of residence or which state's law applies to each of Plaintiffs' common law claims, Apple cannot adequately defend itself, nor can the Court assess the sufficiency of Plaintiffs' claims. Plaintiffs argue their common law claims only under California law, and appear to concede that Plaintiffs wish to proceed under California law. *See* Opp. at 7. In this order, the Court has dismissed Plaintiffs' common law claims with leave to amend. If Plaintiffs file an amended complaint to cure the deficiencies in this order as well as in Apple's motion to dismiss, Plaintiffs should also 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.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS Apple's motion to dismiss without prejudice. Should Plaintiffs elect to file an amended complaint, Plaintiffs shall do so within thirty days of this Order. Failure to file an amended complaint within 30 days or failure to cure the deficiencies identified herein or in Apple's motion to dismiss will result in dismissal with prejudice. Plaintiffs may not add new causes of action or parties without leave of the Court or stipulation of the parties pursuant to Federal Rule of Civil Procedure 15.

IT IS SO ORDERED.

Dated: August 30, 2019

Lucy H. Koh

LUCY H. KOH
United States District Judge