

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

MELISSA BARON, *et al.*,

Plaintiffs,

v.

Case No. 8:21-cv-2349-SCB-SPF

SYNIVERSE CORPORATION,

Defendant.

ORDER

Before the Court is Defendant's Rule 12(b)(1) and Rule 12(b)(6) Motion to Dismiss Plaintiffs' Amended Consolidated Complaint. (Doc. 50). Plaintiffs have filed a response in opposition (Doc. 60), to which Defendant has filed a reply (Doc. 64). Plaintiffs also have filed Notices of Supplemental Authority (Doc. 69, 70), to which Defendant has filed a response (Doc. 73). As explained below, Defendant's Rule 12(b)(1) Motion is granted.

I. BACKGROUND¹

This case is about a cyberattack and data breach that allegedly exposed

¹ The facts that follow are taken from the operative complaint, including quoted portions of a prior iteration of a preliminary proxy statement (the "proxy statement") that Defendant filed with the Securities and Exchange Commission ("SEC") and quoted portions of an article on the data breach. (Doc. 38). Although neither the proxy statement nor the article is attached to the operative complaint, links to access the documents online are cited therein. (*See id.*, pp. 9-14).

mobile phone users’ “private communications.” (Doc. 38, ¶ 1). Syniverse Corporation (“Syniverse” or “Defendant”) is a global telecommunications company whose customers include approximately 800 carriers, including AT&T, T-Mobile, and Verizon. (*Id.*, ¶¶ 5, 29, 31). Syniverse provides network services, outsources carrier solutions, and messaging solutions to its carrier customers, which in turn allows the mobile carriers to “provide their customers with secure global connectivity and messaging.” (*Id.*, ¶ 33). Syniverse processes and routes billions of text messages each year between different carriers and connects billions of devices to the mobile ecosystem. (*Id.*, ¶¶ 3, 33). Its messaging gateways translate mobile carriers’ different protocols to handle incompatibility and route messages across carriers so that end-users can exchange person-to-person (“P2P”) messages between any network or service. (*Id.*, ¶¶ 4-4; Proxy Stmt., p. 266).

Plaintiffs and the Class Members they seek to represent are mobile phone users who sent and received text messages during the times relevant to the data breach. Additionally, Plaintiffs and the Class Members they seek to represent were customers of Syniverse’s customers, namely, AT&T, T-Mobile, and Verizon, during the times relevant to the data breach. (*Id.*, ¶¶ 15-19).

In May 2021, Syniverse discovered that an unknown individual or organization had gained unauthorized access to its operational and information

technology systems beginning in May 2016 (the “Data Breach”). (Doc. 38, ¶ 35). Syniverse conducted an internal investigation, notified law enforcement, commenced remedial actions, and hired specialized counsel. (*Id.*).

On September 27, 2021, Syniverse disclosed the Data Breach to the SEC in connection with a merger. Specifically, it reported to the SEC that:

Syniverse’s investigation revealed that the individual or organization gained unauthorized access to databases within its network on several occasions, and that login information allowing access to or from its Electronic Data Transfer (“EDT”) environment was compromised for approximately 235 of its customers. All EDT customers have been notified and have had their credentials reset or inactivated, even if their credentials were not impacted by the incident. All customers whose credentials were impacted have been notified of that circumstance.

Syniverse has notified all affected customers of this unauthorized access where contractually required, and Syniverse has concluded that no additional action, including any customer notification, is required at this time.

(*Id.*).

One week later, on October 5, 2021, Plaintiffs Melissa Baron, Olivia Enloe, Marco Lerra, and John Pels filed the instant action. (Doc. 1). Two days later, Plaintiffs Alexis Mullen, Nicholas Yeomelakis, and Thomas Macnish filed a nearly identical action. *See Mullen, et al. v. Syniverse Corporation*, No. 8:21-cv-2363-SCB-SPF, (Doc. 1). Plaintiffs in both cases brought claims for negligence, breach of contract, invasion of privacy, and breach of confidence, alleging that Syniverse

failed to properly secure and safeguard their “private and personally identifiable information” (“PII”). Plaintiffs in both cases alleged that their PII included, “without limitation, call records and message data, such as call length and cost, caller[s’] and receivers’ numbers, the location of the parties in the call, as well as the actual content of SMS text messages.”² (Doc. 1, p. 1).

On November 23, 2021, Plaintiffs in this action filed an unopposed motion to consolidate the cases. (Doc. 16). The Court granted the motion and directed Plaintiffs to file a single amended complaint in this case (the lead case). (Doc. 17).

On December 3, 2021, Plaintiffs Melissa Baron, Olivia Enloe, Marco Lerra, John Pels, Alexis Mullen, Nicholas Yeomelakis, and Thomas Macnish filed a six-count consolidated class action complaint. (Doc. 22). Plaintiffs asserted claims for negligence/negligence per se, third-party beneficiary of contracts, breach of implied contract, unjust enrichment, violations of Florida’s Deceptive and Unfair Trade Practices Act (“FDUTPA”), and violations of California’s Consumer Privacy Act. (Doc. 22). Plaintiffs alleged a variety of injuries due to Defendant’s conduct, including expenses associated with identity theft, tax fraud, and unauthorized use of their PII; continued and increased risk to their PII; anxiety and

² Plaintiffs in this action made the above allegations “upon information and belief.” (Doc. 1, p. 1). In the *Mullen* action, Plaintiffs made the above allegations “upon information and belief based upon, inter alia, the investigation of counsel, and review of public documents.” *See Mullen, et al. v. Syniverse Corporation*, No. 8:21-cv-2363-SCB-SPF (Doc. 1).

emotional distress; and loss of privacy. (Doc. 22, ¶¶ 13, 117-18, 126-27, 136-37, 153-55, 167-68). Plaintiffs sought actual, consequential, and nominal damages, as well as injunctive relief. (*Id.*, pp. 49-53).

On January 18, 2022, Defendant filed a motion to dismiss for lack of subject matter jurisdiction and failure to state claims upon which relief could be granted. Among other things, Defendant argued that Plaintiffs lacked standing because they failed to allege any actual or imminent concrete injury and causation. (Doc. 32).

On March 2, 2022, in response to Defendant’s motion to dismiss, Plaintiffs filed an eight-count Amended Consolidated Class Action Complaint (“Amended Complaint” or “Operative Complaint”). (Doc. 38). Plaintiffs bring this action on behalf of all persons whose “private communications were accessed” during the Data Breach as a result of Syniverse’s alleged failure to, among other things, “adequately protect the private communications of Plaintiffs and Class Members.” (*Id.*, ¶¶ 12, 55). As with their prior allegations of PII, Plaintiffs allege “upon information and belief” that their “private communications” were stored on and/or processed through Syniverse’s EDT environment, and include, “without limitation, call records and message data, such as call length and cost, caller and receiver’s numbers, the location of the parties in the call, as well as private communications sent via SMS text messages.” (*Id.*, ¶ 1). In support of their allegations, Plaintiffs

quote heavily from a 2021 article published on VICE.com, which itself quotes several sources when discussing Syniverse’s data breach.³ (See Doc. 38, ¶¶ 36-41 and fn. 9-14). Plaintiffs include the following quotes from the following sources in the Amended Complaint:

1. An unidentified former Syniverse employee:

[Syniverse’s] systems have information on all types of call records.

2. An anonymous telephone carrier employee:⁴

[W]hoever hacked Syniverse could have had access to metadata such as length and cost, caller and receiver’s numbers, the location of the parties in the call, as well as the content of SMS text messages.

Syniverse is a common exchange hub for carriers around the world passing billing info back and forth to each other. . . .So it inevitably carries sensitive info like call records, data usage records, text messages, etc. [. . .] The thing is—I don’t know exactly what was being exchanged in that environment. One would have to imagine though it easily could be customer records and [personal identifying information] given that Syniverse exchanges call records and other billing details between carriers.

3. Karsten Nohlothers, a security researcher:

³ The article is available at: Franceschi-Biccierai, Lorenzo. “Company That Routes Billions of Text Messages Quietly Says It Was Hacked.” *VICE.com, MOTHERBOARD TECH BY VICE*, Oct. 4, 2021, <https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked> (last accessed on Oct. 3, 2022). Additionally, Defendant attaches a copy of the article to its reply. (Doc. 64-1).

⁴ Plaintiffs erroneously attribute the anonymous telephone carrier employee’s statements to the unidentified former Syniverse employee.

Syniverse has access to the communication of hundreds of millions, if not billions, of people around the world. A five-year breach of one of Syniverse's main systems is a global privacy disaster. . . .Syniverse systems have direct access to phone call records and text messaging, and indirect access to a large range of Internet accounts protected with SMS 2-factor authentication. Hacking Syniverse will ease access to Google, Microsoft, Facebook, Twitter, Amazon and all kinds of other accounts, all at once.

4. An anonymous telecom industry insider:

With all that information, I could build a profile on you. I'll know exactly what you're doing, who you're calling, what's going on. I'll know when you get a voicemail notification. I'll know who left the voicemail. I'll know how long that voicemail was left for. When you make a phone call, I'll know exactly where you made that phone call from[.] . . . I'll know more about you than your doctor.

5. Senator Ron Wyden:

The information flowing through Syniverse's systems is espionage gold[.]

That this breach went undiscovered for five years raises serious questions about Syniverse's cybersecurity practices. The FCC needs to get to the bottom of what happened, determine whether Syniverse's cybersecurity practices were negligent, identify whether Syniverse's competitors have experienced similar breaches, and then set mandatory cybersecurity standards for this industry.

(See Doc. 38, ¶¶ 36-41 and fn. 9-14).⁵

⁵ The article contains another quote from the anonymous industry insider, namely, that the data breach *could potentially affect* millions—if not billions—of cellphone users, depending on what carriers were affected[.] It also contains another quote from the former Syniverse employee, who is quoted as stating the following in response to the anonymous industry insider's allegations:

[T]he damage could be much more limited.

I feel it is extremely embarrassing but likely not the cause of significant damage. It

Based on the above, Plaintiffs assert claims for: negligence and negligence per se (Count I); third-party beneficiary of contracts (Count II); breach of implied contract (Count III); unjust enrichment (Count IV); violations of the FDUTPA (Count V); invasion of privacy (Count VI); violations of the California Unfair Competition Law (Unlawful Business Practices) (Count VII); and violations of the California Unfair Competition Law (Unfair Business Practices) (Count VIII).⁶ (*Id.*, ¶¶ 72-161). Plaintiffs allege they “have suffered and will suffer injury,” including the following harms: (1) the continued risk to their private communications (Counts I-III, V-VI);⁷ (2) anxiety and emotional distress (Counts I-II); (3) loss of privacy (Counts I-II); (4) “other economic and non-economic losses” (Counts I-II); (5) the loss of money and property (Counts VII-VIII); and (6) the loss of the legally protected interest in the confidentiality and privacy of their private

strikes me as a result of some laziness, as I have seen security breaches happen like this a few times[.] . . . Because we have not seen anything come out of this over five years. Not saying nothing bad happened but it sounds like nothing did happen. Plaintiffs do not include either of these quotes in the Amended Complaint.

⁶ Counts I-IV are brought on behalf of all Plaintiffs and the Nationwide Class, Count V is brought on behalf Plaintiff Lerra and the Florida Subclass, and Counts VI-VIII are brought on behalf of Plaintiffs Baron and Pels and the California Subclass. (Doc. 38, ¶¶ 72-161).

⁷ Plaintiffs further allege their private communications: “(a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant’s possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the private communications. (Doc. 38, ¶ 12).

communications (Counts VII-VIII). Plaintiffs seek actual, consequential, and nominal damages (Counts I-III, VI); restitution and/or disgorgement (Count IV, VII-VII); and injunctive and/or declaratory relief (Counts III, V-VIII).

Defendant seeks dismissal on two grounds. First, Defendant seeks dismissal under Rule 12(b)(1) for lack of Article III standing. Second, and in the alternative, Defendant seeks dismissal under Rule 12(b)(6) for failure to plead plausible claims for relief. (Doc. 50).

II. LEGAL STANDARDS

A. Standing

Article III of the Constitution “confines the federal judicial power to the resolution of “Cases” and Controversies.” *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). To satisfy the case or controversy requirement, a plaintiff in a matter must have standing to sue. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). In any suit in federal court, therefore, whether a plaintiff has Article III standing to sue presents a threshold jurisdictional question. *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 102 (1998).

Article III standing has three elements: (1) an injury in fact; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely that the

injury will be redressed by a favorable judicial decision.⁸ *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). At the pleading stage, the plaintiff—as the party invoking federal jurisdiction—bears the burden of alleging facts that “plausibly” demonstrate each element. *Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 996 (11th Cir. 2020) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009)). The plaintiff “must demonstrate standing for each claim” asserted and “for each form of relief” sought. *TransUnion*, 141 S. Ct. at 2208.

B. Rule 12(b)(1)

Because a motion to dismiss for lack of standing challenges a court’s subject matter jurisdiction, it is brought under Federal Rule of Civil Procedure 12(b)(1). *Stalley v. Orlando Reg’l Healthcare Sys., Inc.*, 524 F.3d 1229, 1232 (11th Cir. 2008). A defendant can move to dismiss a complaint under Rule 12(b)(1) by asserting a facial and/or factual challenge to subject matter jurisdiction. *Id.* A facial challenge requires the court to determine if the plaintiff has sufficiently alleged a basis for subject matter jurisdiction, and the allegations in the complaint are taken as true for the purposes of the motion. *Id.* at 1232-33. By contrast, a factual challenge contests “the existence of subject matter jurisdiction in fact, irrespective

⁸ While “[t]hese requirements apply with full force in a class action . . . only one named plaintiff must have standing as to any particular claim in order for it to advance.” *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1261 (11th Cir. 2021) (citations omitted).

of the pleadings,” and the court can consider “matters outside the pleadings, such as testimony and affidavits[.]” *McElmurray v. Consol. Gov’t of Augusta-Richmond Cnty.*, 501 F.3d 1244, 1251 (11th Cir. 2007).

III. DISCUSSION

Defendant asserts a facial attack to subject matter jurisdiction, arguing that Plaintiffs lack standing because their injury in fact and causation allegations are facially insufficient. Defendant also asserts a factual attack to subject matter jurisdiction, arguing that the evidence shows that Plaintiffs lack standing because they cannot establish any actual injury. Defendant further argues that to the extent the Court reaches the substance of Plaintiffs’ claims, dismissal is warranted because Plaintiffs fail to allege plausible claims. (Doc. 5).

As explained below, the Court finds that Defendant’s facial challenge to subject matter jurisdiction has merit.⁹ Given this finding, the Court does not reach Defendant’s factual challenge to subject matter jurisdiction, and it lacks jurisdiction to address Defendant’s alternative Rule 12(b)(6) arguments.

⁹ The Court considers the proxy statement and article referenced in the Amended Complaint in ruling on Defendant’s facial challenge. Although those documents are not appended to the Amended Complaint, they are incorporated by reference therein because their contents are central to Plaintiffs’ claims and neither party disputes their contents. *See Wilchombe v. TeeVee Toons, Inc.*, 555 F.3d 949, 959 (11th Cir. 2009); *Maxcess, Inc. v. Lucent Techs., Inc.*, 433 F.3d 1337, 1340 (11th Cir. 2005).

A. Facial Challenge to Injury in Fact

A plaintiff experiences an injury in fact when he or she suffers “an invasion of a legally protected interest” that is both “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560. At issue in this case are whether the injuries alleged are “concrete” and “actual or imminent.”

An injury is concrete if the harm is “real, and not abstract.” *Spokeo*, 578 U.S. at 340. A plaintiff can satisfy the concreteness requirement in one of two ways. First, a plaintiff can allege a direct tangible harm, such as a physical harm or monetary harm. *TransUnion*, 141 S. Ct. at 2204. As discussed below, certain intangible harms can also be concrete. *Id.* Second, a plaintiff can allege a “material” risk of harm. *Equifax*, 999 F.3d at 1262 (quoting *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 927 (11th Cir. 2020)). This is a “high standard” that requires courts to consider the “magnitude of the risk.” *Muransky*, 979 F.3d at 927. When injuries are incurred while mitigating a risk of harm, such as purchasing a credit report or spending time to minimize a risk of identity theft, such injuries necessarily rise or fall along with the determination of whether the alleged risk of harm is a concrete injury. *Equifax*, 999 F.3d at 1262.

As for the actual-or-imminent requirement, when there is no actual injury, a future injury constitutes an Article III injury only “if the threatened injury is certainly impending or there is a substantial risk that the harm will occur;” allegations of possible future injury are insufficient. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014); *Equifax*, 999 F.3d at 1262. If the harm alleged “is not ‘certainly impending,’ or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.” *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1339 (11th Cir. 2021).

1. Injury-in-Fact: Concrete and Actual

In their response, Plaintiffs contend they have standing based on two direct intangible injuries: (1) the disclosure of their private information (text messages and call information), which they also refer to as “intangible privacy harms;” and (2) anxiety and emotional distress resulting from “the exposure of the content of their SMS text messages.”¹⁰ (Doc. 60, pp. 5-10). In support, Plaintiffs rely on *TransUnion*; cases from the Fourth and Seventh Circuits in statutory, non-data

¹⁰ As noted above, Plaintiffs allege in their Amended Complaint that they “have suffered and will suffer injury,” namely: (1) the continued risk to their private communications; (2) anxiety and emotional distress; (3) loss of privacy; (4) “other economic and non-economic losses”; (5) the loss of money and property; and (6) the loss of the legally protected interest in the confidentiality and privacy of their private communications. (Doc. 38).

breach cases; various district court cases; and *Muransky* for the proposition that “very nearly any level of direct injury is sufficient to show a concrete harm.” (Doc. 60, pp. 5-9). In a footnote, Plaintiffs also summarily assert they have standing to bring their claims under California’s Unfair Competition Law (“UCL”) based on their allegation “that Syniverse collected, stored, and then provided substandard protection for” the private communications of Baron, Pels, and the California Subclass. (*Id.*, p. 10 n.4).

Defendant contends that Plaintiffs fail to plausibly allege an injury in fact because their alleged injuries are not “concrete” and “actual or imminent.” The Court agrees. None of Plaintiffs’ alleged harms satisfy the injury in fact requirement of Article III standing.¹¹

a. Disclosure of “private information” (Counts I-III, V-VI)

Plaintiffs fail to plausibly allege that the unauthorized disclosure of their private information (text messages and call information) is itself an intangible harm sufficiently concrete to establish an injury in fact. As noted above, intangible harms can be sufficiently concrete for purposes of Article III standing.

¹¹ The Court also agrees with Defendant that the Amended Complaint presents a threshold fatal deficiency, namely, that Plaintiffs allege throughout that they “have suffered and will suffer” injuries but fail to establish what injuries they have allegedly suffered versus those injuries they allegedly “will suffer” sometime in the future.

TransUnion, 141 S. Ct. at 2204. In *TransUnion*, a case arising under the Fair Credit Reporting Act, the Supreme Court explained:

Various intangible harms can . . . be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion.

Id. To satisfy the concreteness requirement in those instances, a plaintiff must show that the alleged injury “has a ‘close relationship’ to a harm ‘traditionally’ recognized as providing a basis for a lawsuit in American courts.” *Id.* A plaintiff makes that showing by identifying “a close historical or common-law analogue for their asserted injury.” *Id.* Relevant here, the Supreme Court in *TransUnion* added that when an element “essential to liability” at common law is missing from an alleged harm, the common-law comparator is not closely related to that harm. *Id.* at 2209-10; *see also Muransky*, 979 F.3d at 932. In other words, a theory that “circumvents a fundamental requirement” of an analogous common-law tort “does not bear a sufficiently ‘close relationship’” to establish standing. *TransUnion*, 141 S. Ct. at 2210 n.6.

Such is the case here. Plaintiffs contend they make this showing because their alleged intangible injury—the unauthorized disclosure of their private information due to the data breach—has a close common-law analogue, namely,

the tort of public disclosure of private information. Stated differently, Plaintiffs contend the unauthorized disclosure of their text messages/call logs is an intangible harm that bears a close relationship with the tort of public disclosure of private information. Plaintiffs, however, do not plead that kind of harm in the Amended Complaint.

The public disclosure tort allows a plaintiff to sue when someone “gives publicity to a matter concerning [his] private life.” Restatement (Second) of Torts § 652D (Am. L. Inst. 1977). “Publicity” means that “the matter is made public by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.” *Id.* § 652D cmt. a. Such publicity causes the plaintiff to suffer an “invasion of his privacy.” *Id.* § 652D. In this case, Plaintiffs fail to allege that Defendant or the hacker(s) communicated their private information to the public at large or to so many people that the content of their text messages and call logs are certain to become public knowledge. Because Plaintiffs do not allege publicity, they do not plead the kind of harm that the public disclosure tort is aimed at redressing, and they fail to satisfy the concreteness requirement in this manner. *See, e.g., Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, ___ F.4th ___, 2022 WL 4102824, at *2 (11th Cir. Sept. 8, 2022) (concluding, in a statutory case, that there was no concrete

injury based on the asserted harm being adequately analogous to the harm recognized by the tort of public disclosure of private information because the plaintiff had not alleged the element of publicity).

Moreover, none of the cases Plaintiffs cite in their Response provide a basis for the Court to conclude otherwise. Plaintiffs cite Fourth and Seventh Circuit authority, as well as several district-court cases, that rely on *TransUnion* for the proposition that an unauthorized disclosure of personal information is a concrete harm sufficient on its own for purposes of standing because it amounts to an invasion of privacy. (*See* Doc. 60, pp. 5-10). While some of the cases provide support for Plaintiffs' position, none of the cases are binding on this Court and Plaintiffs did not mention or discuss the import of the Eleventh Circuit's decisions in *Tsao* or *Hunstein*. Likewise, none of the cases Plaintiffs cite in their Notices of Supplemental Authority compel a finding that the alleged intangible injury is sufficiently concrete. Rather, those cases involved disclosure of PII, not text message communications or call records, and none of the cases are controlling authority.¹²

¹² Plaintiffs cite *Clemens v. ExecuPharm Inc.*, ___ F. 4th ___, 2022 WL 4005322, at *9 (3d Cir. Sept. 2, 2022); *Leonard v. McMenamins, Inc.*, 2022 WL 4017674, No. 2:22-cv-00094-BJR, at *4-5 (W.D. Wash. Sept. 2, 2022); *In re USAA Data Security Litigation*, 2022 WL 3348527, at *5 (S.D.N.Y. August 12, 2022); and *Wynne v. Audi of America*, No. 21-cv-08518-DMR, 2022 WL 2916341, at *4-5 (N.D. Cal. July 25, 2022). (Docs. 69, 70).

For these reasons, this Court finds that Plaintiffs’ allegations as to the unauthorized disclosure of their text messages and call records due to the data breach do not bear a sufficiently close relationship to the type of harm protected by the tort of public disclosure of private information. As such, Plaintiffs fail to satisfy the concreteness requirement.

b. Anxiety and Emotional Distress (Counts I and II)

Plaintiffs fail to plausibly allege a concrete harm by virtue of their alleged anxiety and emotional distress. First, Plaintiffs’ blanket allegations of “anxiety, emotional distress,” without more, are too conclusory. *See Iqbal*, 556 U.S. at 678 (The allegations must contain more than “an unadorned, the-defendant-unlawfully-harmed-me-accusation”). Second, given the finding above that Plaintiffs fail to plausibly allege that the disclosure of their private information is a concrete harm, their alleged anxiety and emotional distress arising from that harm, standing alone, are not intangible harms sufficiently concrete to confer standing. Absent a showing that the unauthorized disclosure of their text messages and call information is an intangible harm sufficiently concrete to confer standing, Plaintiffs’ allegation of emotional harm resulting from the same also fails to confer standing. *See, e.g., Equifax*, 999 F.3d at 1262; *Preisler v. Eastpoint Rec. Grp., Inc.*, 2021 WL

2110794, at *5 (S.D. Fla. May 25, 2021) (a plaintiff “cannot rely solely on his feelings of distress, confusion, or anxiety to fabricate concrete injury”).

c. Loss of Money and Property (Counts VII and VIII)

Plaintiffs fail to plausibly allege an injury in fact (and causation) under California’s UCL. The UCL provides a cause of action for business practices that are (1) unlawful; (2) unfair; or (3) fraudulent. Cal. Bus. & Prof. Code § 17200, *et seq.* To have standing, a plaintiff must allege that (1) he or she has “lost ‘money or property’ sufficient to constitute an ‘injury in fact’ under Article III of the Constitution” and 2) there is a “causal connection” between the defendant’s alleged UCL violation and the plaintiff’s injury in fact. *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203-04 (9th Cir. 2010) (citations omitted); *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 322 (Cal. 2011). A plaintiff may show an economic injury from unfair competition in a number of ways. A plaintiff may: (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary. *Kwikset Corp.*, 51 Cal. 4th at 323.

In the Amended Complaint, Plaintiffs allege that as a direct and proximate result of Syniverse’s “acts of unfair practices” and “unlawful practices and acts”:

Plaintiffs Baron and Pels and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of the California Subclass’s legally protected interest in the confidentiality and privacy of their private communications, nominal damages, and additional losses as described above.

(Doc. 38, ¶¶ 153, 159). These allegations fail to adequately allege a loss of money or property due to Syniverse’s alleged UCL violations. Notably, Plaintiffs do not articulate that they paid Syniverse anything for its services, the nature of Syniverse’s services, or how Syniverse’s conduct plausibly caused Baron or Pels to lose money or property.¹³ As such, Plaintiffs’ allegations are too vague, unsupported, and conclusory to state a plausible injury or causation under the UCL. *See, e.g., Iqbal*, 556 U.S. at 678 (“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.”); *Hosseini v. Wells Fargo Bank, N.A.*, 2013 WL 4279632, at *8 (N.D. Cal. Aug. 9, 2013) (rejecting the “conclusory allegation that [the plaintiffs] ‘were injured in fact and lost money or property as a result’ of Defendant’s ‘practices’”); *Baird v. Sabre Inc*,

¹³ Nor do Plaintiffs cite any authority in their response supporting their assertion of standing under the UCL.

2013 WL 12130570, at *3 (C.D. Cal. May 8, 2013) (dismissing the plaintiff’s UCL claim where she could not “articulat[e] [] how” the alleged conduct caused her injury). Further, Plaintiffs’ allegation of the loss of their legally protected interest in the confidentiality and privacy of their private communications is not an economic injury for purposes of the UCL. *See In re Facebook Privacy Litig.*, 572 F. App’x 494 (9th Cir. 2014); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 862-63 (N.D. Cal. 2011).

2. Injury-in-fact: Concrete and Imminent

Plaintiffs fail to plausibly allege a concrete, imminent future injury. “[T]o demonstrate that a case or controversy exists to meet the Article III standing requirement when a plaintiff is seeking injunctive or declaratory relief, a plaintiff must allege facts from which it appears there is a substantial likelihood that he will suffer injury in the future.” *AA Suncoast Chiropractic Clinic, P.A. v. Progressive Am. Ins. Co.*, 938 F.3d 1170, 1179 (11th Cir. 2019) (quoting *Malowney v. Fed. Collection Deposit Grp.*, 193 F.3d 1342, 1346-47 (11th Cir. 1999)). “An allegation of future injury may suffice if the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk that the harm will occur.’” *Susan B. Anthony List*, 573 U.S. at 158 (quoting *Clapper*, 568 U.S. at 414 n.5). “The controversy between the

parties cannot be ‘conjectural, hypothetical, or contingent; it must be real and immediate, and create a definite, rather than speculative threat of future injury.’” *A&M Gerber Chiropractic LLC v. GEICO Gen. Ins. Co.*, 925 F.3d 1205, 1210 (11th Cir. 2019) (quoting *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985)). Allegations “of possible future injury are not sufficient.” *Clapper*, 133 S. Ct. at 1147; *see also Emory*, 756 F.2d at 1552 (“The remote possibility that a future injury may happen is not sufficient to satisfy the ‘actual controversy’ requirement for declaratory judgments.”).

In their response, Plaintiffs contend they have alleged an imminent injury sufficient to confer Article III standing, namely, “the use of information contained in their text messages, call logs, and other information exposed in the data breach because such data contains private information.”¹⁴ (Doc. 60, p. 10). Plaintiffs argue that Syniverse’s contention, *i.e.*, there is no imminent injury because no harm has occurred in almost six years, is not persuasive because Syniverse acknowledged in its Proxy Statement that there is a “possibility” of a present or future imminent injury resulting from the Data Breach. (*Id.*, pp. 11-12).

¹⁴ In support, Plaintiffs rely exclusively on *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015).

Plaintiffs' allegation of possible future harm is dependent on a speculative chain of possibilities and, thus, is insufficient to confer standing. *See Clapper*, 568 U.S. at 401 (“[R]espondents’ theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending’”). At a minimum, for this alleged future harm to occur, the hacker(s) would have to have obtained the content of Plaintiffs’ text communications and/or call logs, somehow identified the individual Plaintiffs from that information, and then used that information to commit identity theft or fraud against Plaintiffs. The fact that over six years have passed since the beginning of the Data Breach and no Plaintiffs have alleged instances of identity theft or fraud only serves to underscore the speculative nature of Plaintiffs’ allegation.

Plaintiffs’ allegation of possible future harm is also conclusory and supported only by Syniverse’s alleged acknowledgement that the risk is “possible” and statements by anonymous individuals and one researcher that the Data Breach could result in identity theft or fraud. Notably, the statements made by the unidentified former Syniverse employee undercut Plaintiffs’ claim of an imminent future injury. The unidentified former Syniverse employee stated only that the EDT “systems have information on all types of call records.” (Doc. 64-1, p. 4). While Plaintiffs attribute another statement to the unidentified former Syniverse

employee, namely, that “whoever hacked Syniverse could have had access to metadata such as length and cost, callers’ and receivers’ numbers, the location of the parties in the call, as well as the content of SMS text messages,” (*see* Doc. 38, ¶ 36), that statement was made by an “anonymous” individual who “works at a telephone carrier” (*see* Doc. 64-1, p. 5). Notably, that anonymous individual later admitted that “I don’t know exactly what was being exchanged in that [EDT] environment.” (*Id.*). Also telling is that Plaintiffs ignored the unidentified Syniverse employee’s statements on the damage potential of the Data Breach:

[T]he damage could be much more limited.

I feel it is extremely embarrassing but likely not the cause of significant damage. It strikes me as a result of some laziness, as I have seen security breaches happen like this a few times[.] . . . Because we have not seen anything come out of this over five years. Not saying nothing bad happened but it sounds like nothing did happen.

(Doc. 64-1, p. 8). As for the other statements quoted in the article that Plaintiffs included in the Amended Complaint, namely, those from a security researcher, an unidentified “telecom industry insider,” and Senator Ron Wyden, those statements are conclusory and rest entirely on speculation. And conclusory allegations of an elevated or continuing risk of injury are not enough to confer standing. *See Tsao*, 986 F.3d 1343; *Muranksy*, 979 F.3d at 933.

Additionally, Plaintiffs' failure to identify any misuse of their personal private communications or data weighs against finding a substantial risk of imminent injury. *See Stapleton on behalf of C.P. v. Tampa Bay Surgery Ctr., Inc.*, 2017 WL 3732102, at *3 (M.D. Fla. Aug. 30, 2017); *see also In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 955 (D. Nev. 2015) (recognizing that the majority of courts dealing with data-breach cases post-*Clapper* have held that absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing). Although actual identity theft or misuse of their data is not required, Plaintiffs' failure to allege either renders their allegation of possible future harm less plausible.

Plaintiffs' allegation of an imminent future injury is also unsupported by Eleventh Circuit authority. In *Equifax*, a data breach exposed "at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers." 999 F.3d at 1262. The plaintiffs claimed that "identity thieves" could use this information to "create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness." *Id.* They also alleged that they "'remain[ed] subject to a pervasive, substantial and imminent risk of identity theft and fraud' due to the 'highly-

sensitive nature of the information stolen,’ and that they spent time, money, or effort dealing with the breach.” *Id.* The Eleventh Circuit held that, “[g]iven the colossal amount of sensitive data stolen, including social security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data,” the plaintiffs “adequately alleged that they face a ‘material’ and ‘substantial’ risk of identity theft that satisfies the concreteness and actual-or-imminent elements.” *Id.* The same conclusion does not follow here.

Unlike the plaintiffs in *Equifax*, Plaintiffs allege that unauthorized persons obtained *unspecified* “information contained in their text messages, call logs, and other information exposed” in the Data Breach. Plaintiffs do not allege what information was contained in their text messages or that their text messages and call logs contained PII, such as birthdates or social security numbers. Nor do Plaintiffs plausibly allege that the “private information” contained in their text messages or call logs is the type of information that subjects them to a substantial or imminent risk of identity theft or fraud. Although Plaintiffs attempt to do so by quoting the statements made by anonymous persons and a researcher in the cited article, such statements fall short of showing an imminent future injury. To the extent Plaintiffs rely on Syniverse’s “acknowledgement” in the Proxy Statement, the acknowledgement at most supports only the possibility of future injury, not that

a future injury is imminent.

For the reasons set forth above, Plaintiffs fail to plausibly allege an imminent future injury sufficient to confer Article III standing.

B. Facial Challenge to Causation

Given the findings above, the Court need not address the causation or traceability requirement. However, even if Plaintiffs plausibly alleged a concrete actual or imminent injury, Plaintiffs' allegation that Syniverse's substandard security allowed the data to be accessed by unauthorized third parties does not satisfy the causation or traceability requirement.

Article III demands an injury that is "fairly traceable to the challenged conduct of the defendant." *Spokeo*, 136 S. Ct. at 1547. Traceability requires a "causal connection between the injury and the conduct complained of." *Focus on the Family*, 344 F.3d at 1273. A traceability showing need not rise to the level of proximate causation; even an indirect injury can satisfy the requirement. *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1271 (11th Cir. 2019). However, the injury must result from the conduct of the defendant—and not "some third party." *Lujan*, 504 U.S. at 560. The main inquiry is whether "the line of causation between the illegal conduct and injury [is] too attenuated" to establish traceability. *Allen v.*

Wright, 468 U.S. 737, 752, *abrogated on other grounds by Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118 (2014).


Here, any harm that could occur arguably was caused by a third-party not before the Court and, therefore, is not traceable to Syniverse's alleged conduct. Alternatively, the traceability between Syniverse's conduct and the injury is too attenuated.

IV. CONCLUSION

In accordance with the foregoing, it is **ORDERED** and **ADJUDGED**:

1. Defendant's Rule 12(b)(1) Motion to Dismiss Plaintiffs' Amended Consolidated Complaint (Doc. 50) is **GRANTED**.
2. Plaintiffs' Amended Consolidated Class Action Complaint (Doc. 38) is **DISMISSED without prejudice** for lack of subject-matter jurisdiction.¹⁵
3. Plaintiffs may have 30 days to file an amended complaint that alleges an injury in fact and causation, if Plaintiffs are able to do so. Failure to file an amended complaint within 30 days will result in this case being closed without further notice.

DONE AND ORDERED at Tampa, Florida, this 7th day of October 2022.



SUSAN C. BUCKLEW
United States District Judge

¹⁵ "A dismissal for lack of subject matter jurisdiction is not a judgment on the merits and is entered without prejudice." *Stalley*, 524 F.3d at 1232; see *Warth v. Seldin*, 422 U.S. 490, 501 (1975) (noting that where defendant successfully challenges plaintiff's standing at pleading stage, district courts ordinarily should afford plaintiff leave to amend).