UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

ANGELICA DIPIERRO, et al.,
on behalf of themselves and all
others similarly situated,

Plaintiffs,

v. Case No: 8:23-cv-01864-KKM-NHA

FLORIDA HEALTH
SCIENCES CENTER, INC.,

Defendant.

ORDER

Angelica DiPierro, Stacey Graham, Deborah Ivey, Edward James, Sr., Keon Critchlow, and Aubrey Rassel sue Tampa General Hospital on their own behalf and as proposed representatives of a nationwide class. *See* Am. Compl. (Doc. 8). Based on a May 2023 data breach, Plaintiffs allege common law tort and contract claims as well as violations of the Florida Deceptive and Unfair Trade Practices Act (FDUTPA). Am. Compl. ¶¶ 185–243. Plaintiffs now move for preliminary certification of their class and for preliminary approval of a class-wide settlement. Mot. for Prelim. Approval (MPA) (Doc. 37). After careful consideration, I conclude that no named Plaintiff has standing. Accordingly, I remand the case to state court for lack of subject matter jurisdiction.

I. BACKGROUND

Tampa General "is a private, not-for-profit hospital headquartered in Tampa, Florida." Am. Compl. ¶ 39. Between May 12 and May 30, 2023, Tampa General's computer systems experienced a data breach. *Id.* ¶¶ 3, 51. During the incident, an unauthorized third party infiltrated Tampa General's systems and obtained access to certain files, which included "some patient information" from a group of roughly 2.1 million[1] individuals. *Id.*; *see also id.* ¶ 4 (alleging that "names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by [Tampa General] for its business operations" were "stolen"). On May 31, 2023, Tampa General learned of the incident and started investigating. Am. Compl. ¶¶ 3, 5. On July 19, 2023, Tampa General began issuing "Cybersecurity Notice[s]" informing potentially affected individuals of what had happened. *Id.* ¶ 51.[2]

[1] The amended complaint states that "[Tampa General's] investigation concluded that the Private Information compromised in the Data Breach included Plaintiffs' and approximately 1.2 million other individuals' information." Am. Compl. ¶ 5; *see also id.* ¶¶ 9, 177. But the motion for preliminary approval and the settlement agreement each indicate over two million class members. *See* MPA at 19 (explaining that numerosity is met because there are "approximately two million Settlement Class Members"); Settlement Agreement (Doc. 37-1) at 2–3 (explaining that "[Tampa General's] investigation confirmed the [data breach] included approximately 2.1 million individuals' Personally Identifiable Information"). Because the greater number of class members is used in the settlement agreement and in Plaintiffs' most recent filings, I rely on it.

[2] Appendix A reflects the full text of Tampa General's cybersecurity notice as it currently appears.

Relying on the cybersecurity notice posted online, Plaintiffs allege that a laundry list of private information was stolen from each class member. *See* Am. Compl. ¶ 4 n.3 (citing TAMPA GEN. HOSP., *Cybersecurity Notice: Notice to Our Patients of Cybersecurity Event* (*Cybersecurity Notice*) (last visited June 18, 2024), https://perma.cc/3D3F-GDR3; *see also id.* ¶ 51 (quoting same)). But the cybersecurity notice itself equivocates, explaining that, although Tampa General "reviewed the files involved and determined that *some* patient information was included," "[t]he information *varied by individual*" and only "*may* have included" the listed pieces of information. *See Cybersecurity Notice* (emphasis added). Tampa General also hedged on whether any given individual's information had been stolen. *See id.* (explaining that it would "be mailing notification letters to *individuals whose information may have been involved*" and "providing individuals whose Social Security number was involved with complimentary credit monitoring and identity theft protection services" (emphasis added)).

Two days after Tampa General posted the first cybersecurity notice, Plaintiffs sued in the Thirteenth Judicial Circuit Court in and for Hillsborough County, Florida. *See* Class Counsel Decl. (Doc. 37-2) ¶ 4. Plaintiffs are patients who contracted with Tampa General for healthcare services and provided the hospital with their private information during treatment. *See* Am. Compl. ¶¶ 11–34. Plaintiffs allege that their information was stolen during the data breach and that they believe the information has

been or will be sold on the dark web, consistent with hackers' modus operandi. *Id.* ¶¶ 53–54, 59, 120. They claim that Tampa General's failure to employ reasonable data security practices and procedures allowed the data breach to occur. *Id.* ¶ 52.

More than a dozen similar suits were filed, most of which were later removed to federal court and then transferred to me. All but one of the related federal actions were stayed pending mediation in this first-filed case. The Parties attended mediation and agreed on the terms of a proposed global settlement. *See generally* Notice of Settlement (Doc. 31). About two months later, the Parties finalized their agreement and submitted the settlement for preliminary class certification and approval. *See generally* MPA; Settlement Agreement (Doc. 37-1).

II. LEGAL STANDARD

Section 1447(c) of Title 28 provides that, in an action removed to federal court, "[i]f at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." Thus, "[w]hen a case is removed from state to federal court and the plaintiffs do not have Article III standing in federal court, the district court's only option is to remand back to state court." *See Ladies Mem'l Ass'n, Inc. v. City of Pensacola*, 34 F.4th 988, 994 (11th Cir. 2022).

III. ANALYSIS

Plaintiffs request that I certify a single preliminary class for purposes of settlement of "all persons in the United States who were sent notification from [Tampa General] that their Private Information[3] *was potentially compromised* as a result of the [data breach]." *See* MPA at 7 (emphasis added); Settlement Agreement ¶ 51.[4] They also request that I approve the settlement agreement under Federal Rule of Civil Procedure Rule 23 on a preliminary basis. In evaluating the motion to preliminarily certify to settle, several standing problems became evident. Because I conclude that none of the named Plaintiffs have Article III standing, I remand the case to state court for lack of subject matter jurisdiction. *See* 28 U.S.C. § 1447(c); *Ladies Mem'l Ass'n*, 34 F.4th at 994. I also explain why, even if one named Plaintiff had standing, class-wide standing concerns would likely pose substantial predominance problems preventing preliminary class certification.

A. Article III Standing

Standing is a threshold issue in every federal case, and a federal court must evaluate a plaintiff's standing throughout the litigation to ensure that the court maintains subject

[3] The settlement agreement uses the blanket phrase "Private Information" to refer to two categories of information—"Personally Identifiable Information" and "Protected Health Information," which together includes "names, addresses, telephone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by [Tampa General] for its business operations." *See* Settlement Agreement ¶ 2.

[4] The amended complaint asserts two classes, one nationwide and one limited to Florida residents. *See* Am. Compl. ¶ 174. Both the settlement agreement and the motion for preliminary certification and approval identify only a nationwide class. *See* MPA at 7; Settlement Agreement ¶ 51.

matter jurisdiction. *See, e.g.*, *Smith v. GTE Corp.*, 236 F.3d 1292, 1299 (11th Cir. 2001) ("[A] court must zealously insure that jurisdiction exists over a case, and should itself raise the question of subject matter jurisdiction at any point in the litigation where a doubt about jurisdiction arises."). Not only is standing an ongoing burden, "a plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is sought." *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008) (citations and quotations omitted). He does so by establishing that he: "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

"By limiting who can sue, the standing requirement implements 'the Framers' concept of the proper—and properly limited—role of the courts in a democratic society.' " *FDA v. All. for Hippocratic Med.*, No. 23-235, slip op. at 7 (2024) (quoting J. Roberts, *Article III Limits on Statutory Standing*, 42 DUKE L. J. 1219, 1220 (1993)). Enforcement of "the standing requirement means that the federal courts may never need to decide some contested legal questions," instead reserving them "to the political processes." *Id.* This is a feature of our constitutional system, not a bug. The separation of powers, the "single basic idea" that underwrites standing doctrine, *see id.* at 5 (quoting *United States v. Texas*, 599 U.S. 670, 675 (2023)), "was not simply an abstract generalization in the minds of the

Framers: it was woven into the document that they drafted in Philadelphia in the summer of 1787." *Id.* (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 422–23 (2021)).

In class actions, these requirements are temporarily abated by the "basic principle that at the class certification stage only the named plaintiffs need have standing." *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 888 (11th Cir. 2023) (footnote omitted); *see also In re Equifax Inc. Customer Data Sec. Breach Litig.* (*Equifax*), 999 F.3d 1247, 1261 (11th Cir. 2021) ("[O]nly one named plaintiff must have standing as to any particular claim in order for it to advance."). Nonetheless, "[e]very class member must have Article III standing in order to recover individual damages. Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not." *TransUnion*, 594 U.S. at 431 (quotations omitted).

The amended complaint suffers from several standing problems. I discuss each in turn.

1. The Standard of Proof for Standing at the Preliminary Certification Stage of a Certification-for-Settlement Case

Preliminary certification of a class for purposes of settlement initiates a process that aims to produce a final order granting class members individual relief. With that immediate goal at hand, applying only the "one named plaintiff" principle of standing and the Federal Rules of Civil Procedure's pleading standards makes little sense. Doing so merely delays the threshold jurisdictional question until the fairness hearing or thereabout, but without

allowing for meaningful discovery or other trial-related preparation in the interim to establish standing for all class members.

The concern can be seen in an example: Were this case to proceed to final judgment after a trial, "the specific facts set forth by [Plaintiffs] to support standing" would need to "be supported adequately by the evidence adduced." *TransUnion*, 594 U.S. at 431 (citations and quotations omitted). At the final judgment stage, pleadings of course would not suffice. That the parties might agree to certify a class to achieve a global settlement and secure a final judgement via that route does not negate this jurisdictional hurdle. Indeed, the constitutional necessity that each plaintiff must prove standing before he is awarded relief creates some tension with the general idea of a certification-for-settlement class, the basic purpose of which is to permit quick(er) mass litigation under appropriate circumstances but without the attendant discovery and trial burdens.

Considering the open question of what standard of proof for standing is required at the certification-to-settle stage brings this tension into focus. *TransUnion* reserved "the distinct question whether every class member must demonstrate standing *before* a court certifies a class." *Id.* at 431 n.4 (citing *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1277 (11th Cir. 2019) ("A plaintiff need not prove that every member of the proposed class has Article III standing prior to certification, and in some cases a court might reasonably certify a class that includes some putative members who might not have satisfied the requirements

of *Lujan* and decide to deal with the problem later on in the proceeding, but before it awarded any relief.")). Accordingly, the Supreme Court has never explained the burden of proof required to demonstrate standing in the certification-for-settlement context. *See Williams v. Reckitt Benckiser LLC*, 65 F.4th 1243, 1254 (11th Cir. 2023) (explaining that the burden is "unclear"). Faced with this uncertainty, the Eleventh Circuit has "assume[d] without deciding that the applicable standard [for demonstrating standing in such cases] is a pleading standard." *Id.*; *see also Smith v. Miorelli*, 93 F.4th 1206, 1212 n.7 (11th Cir. 2024) (assuming the same).

Plaintiffs do not address this concern or explain why a greater standard of proof should not apply to preliminary class certification when the sole purpose is to achieve a global settlement, *i.e.,* a final judgment awarding relief to the entire class. *See TransUnion*, 594 U.S. at 431 ("Every class member must have Article III standing in order to recover individual damages."); *Cordoba*, 942 F.3d at 1274 ("The essential point . . . is that at some time in the course of the litigation the district court will have to determine whether each of the absent class members has standing before they [can] be granted any relief."). Instead, they contend that "[t]here is no requirement that Article III standing be proved with evidentiary support at the settlement approval stage," drawing on a footnote in a pre-*TransUnion* decision. *See* MPA at 16 (citing *Equifax*, 999 F.3d at 1261 n.8). This argument overreads Eleventh Circuit precedent. Although *Equifax* appeared skeptical that

"Plaintiffs were required to prove they had Article III standing with evidentiary support at the final approval stage," that opinion then stated that it "need not decide th[e] issue" because there was no factual challenge to standing. *Equifax*, 999 F.3d at 1261 n.8. The Eleventh Circuit's recognition in *Williams* and *Smith* (as informed by the Supreme Court's intervening decision in *TransUnion*) that the standard of proof for demonstrating standing in a certification-for-settlement case is "unclear," combined with those decisions' express reservation of the issue, forecloses Plaintiffs' broad reading of *Equifax*.

For purposes of the standing analysis below, I assume that a pleading standard applies. But the bottom line remains: Before I award any class member final relief, that member must have standing. *See TransUnion*, 594 U.S. at 431; *Cordoba*, 942 F.3d at 1274. Plaintiffs seem to assume that I can preliminarily approve their settlement agreement based on a pleading standard and then never explain how or when I would revisit their burden to establish standing for each class member with evidence before entering a final judgment. This proposal raises constitutional concerns and is also particularly relevant to the predominance inquiry under Rule 23(b)(3). *See Cordoba*, 942 F.3d at 1272–77. Thus, even if I did not remand the case to state court for lack of standing, further inquiry into the standard of proof would be prudent before I would preliminarily certify any class or approve any class settlement.

2. Data Breach Standing Principles

A plaintiff must allege an "injury in fact that is concrete, particularized, and actual or imminent" to plead the first element of standing. *TransUnion*, 594 U.S. at 423 (citing *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 560–61 (1992)). A concrete injury can be tangible—like a physical or monetary harm—or intangible—like harm to one's reputation. *Id.* at 425. A harm is "actual" if it has already occurred, but a risk of future harm does not give rise to standing unless the risk is "sufficiently imminent and substantial." *Id.* at 435 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414, n.5 (2013)). Each kind of harm has its own analytical framework, and a plaintiff's proffered harms must be analyzed on a claim-by-claim, harm-by-harm basis. *See, e.g.*, *Green-Cooper*, 73 F.4th at 889 ("[A] mere risk of future harm, without more, does not give rise to Article III standing for recovery of damages, even if it might give rise to Article III standing for purposes of injunctive relief.").

"For purposes of the concrete injury analysis under Article III, [the Eleventh Circuit] ha[s] recognized three kinds of harm: 1) tangible harms, like physical or monetary harms; 2) intangible harms, like injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts; and, finally, 3) a material risk of future harm when a plaintiff is seeking injunctive relief." *Id.* (cleaned up). Of course, as a technical matter, the third category of concrete harm is simply a sufficiently imminent risk of one of the first two kinds of harm manifesting.

Applying these principles in data breach litigation, the Eleventh Circuit has held that "a plaintiff whose personal information is subject to a data breach can establish a concrete injury for purposes of Article III standing if, as a result of the breach, he experiences 'misuse' of his data in some way." *Id.* (quoting *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021)). Misuse can constitute both a present intangible injury and an imminent risk of tangible injury in the future. *See id.* at 889–90, 890 n.9. For example, a plaintiff whose "credit card data and corresponding personal information" is placed for sale on the dark web may seek damages and forward-looking relief because that kind of misuse "establishes both a present injury—credit card data and personal information floating around on the dark web—and a substantial risk of future injury—future misuse of personal information associated with the hacked credit card." *Id.* at 889–90.

To determine whether the named Plaintiffs or the class have standing, I must analyze each harm alleged in the amended complaint under this rubric.

3. Plaintiffs' Class-Wide Injury Arguments

Even assuming the most generous standard of proof (plausibility under Federal Rule of Civil Procedure 8(a)(2)), the amended complaint does not establish that each (or any) member of the class has suffered an injury in fact. At a high level of generality, Plaintiffs argue that the entire class has suffered an Article III injury because the class's "Private

Information was allegedly impacted in the [data breach] when an unauthorized third party gained access to [Tampa General's] files containing its patients' sensitive and confidential information." MPA at 16. Plaintiffs have developed several variations of this argument based on different harms. *See id.* at 16–18; Resp. to MTD (Doc. 29). But none establish that the class has, collectively, suffered a concrete injury or is at substantial risk of future harm.

i. Increased Risk of Future Harm and Time and Effort Mitigating that Risk

Plaintiffs' first theory of standing is that the data breach "caused them harm including (1) a substantial increased risk of fraud and identity theft, and (2) time spent dealing with the Data Breach's consequences." Resp. to MTD at 5–7. While both fraud and the loss of one's time are tangible and therefore concrete, the allegations here are neither actual nor imminent for purposes of Article III.

A risk of future harm and a self-inflicted injury designed to mitigate that risk are "inextricably tied" together, and thus rise or fall as one for standing purposes. *Tsao*, 986 F.3d at 1344. In other words, a plaintiff's "management-of-risk claim is bound up with his arguments about actual risk." *Muransky v. Godiva Chocolatiers, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc). The key for both, including in data breach litigation, is whether the risk of future harm is sufficiently substantial and imminent. "[I]f the hypothetical 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 [himself] to mitigate [the] perceived risk." *Tsao*, 986 F.3d at 1339 (quotations omitted). Thus, determining whether Plaintiffs have alleged sufficient facts to plausibly plead a concrete risk of future harm resolves any related issues about expenditure of time and effort to mitigate against that future harm.

In *Tsao*, after surveying the decisions of eight other circuits, the Eleventh Circuit promulgated a test for analyzing this fact pattern. *See id.* at 1340–44. In short, "evidence of actual misuse is not necessary for [an individual] plaintiff to establish standing following a data breach." *Id.* at 1343. But plaintiffs must identify "specific evidence of *some* misuse of class members' data" to plead a substantial risk of future harm. *Id.* at 1344. "[V]ague, conclusory allegations that members of the class have suffered" misuse do not suffice, even under a plausibility standard. *See id.* at 1343 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

The precise definition of "misuse," and the necessary quantum of evidence required to show a substantial, class-wide risk of future harm, remain open questions. The answers to these questions should reflect the limited role of federal courts in our system of constitutional government and ensure that federal courts decide cases only where plaintiffs have suffered real harm (or are at substantial risk of future harm). *See TransUnion*, 594 U.S. at 422–24. Courts concerned with safeguarding that limited role should take care to

resolve remaining questions about the nature and quantum of required misuse in data breach litigation to avoid definitions of misuse that would oblige the judiciary to "exercise general legal oversight . . . of private entities" based on a "roving commission to publicly opine on every legal question." *Id.* at 423–24; *cf. id.* at 434 ("A letter that is not sent does not harm anyone, no matter how insulting the letter is. So too here."). Notwithstanding this uncertainty, *Tsao*, *Equifax*, and *Green-Cooper* provide helpful touchstones to guide the inquiry.

Tsao was an easy "no standing" case. There, the district court concluded that Tsao lacked standing because he failed to "identify a single specific, concrete injury in fact that he or anyone else suffered as a result of any misuse of customer credit card information" following the data breach. *Id.* at 1337 (cleaned up). The Eleventh Circuit agreed, explaining that "Tsao offer[ed] only vague, conclusory allegations that members of the class ha[d] suffered any actual misuse of their personal data—[t]here, 'unauthorized charges.' " *Id.* at 1343. Such "conclusory allegations of injury" could not confer standing based on the future risk of identity theft absent "specific evidence of some misuse of class members' data." *Id.* at 1343–44.

Green-Cooper presented a straightforward case in the opposite direction. There, the plaintiffs alleged "that their credit card and personal information was 'exposed for theft and sale on the dark web.' " 73 F.4th at 889. The allegation was much more specific than

Tsao's vague claims about "unauthorized charges," with the plaintiffs "explain[ing] that, based on [the Defendant's] internal reporting, the information for *all* 4.5 million cards the hackers accessed in the Brinker system were found on Joker Stash," a specific dark web marketplace. *Id.* at 886–87 (emphasis added). This "critical" allegation—"that hackers took credit card data and corresponding personal information from [the Defendant's] systems and affirmatively posted that information for sale on Joker Stash"—was "the misuse for standing purposes that . . . was missing in *Tsao*." *Id.* at 889–90 (footnote omitted). The Eleventh Circuit had no need to wrestle with the difficulties presented when (1) a named plaintiff's factual allegations do not specify whether all of the class's information was stolen and (2), even if alleged as stolen, whether all of the class's information was posted for sale.

Equifax is an example of a less clear-cut case. There, "dozens of Plaintiffs allege[d] they ha[d] already had their identities stolen and thus suffered injuries in many different ways," including actual fraud. 999 F.3d at 1262–63. Although dozens of instances of misuse may not seem like much compared to a "class of approximately 147 million members," *id.* at 1267, the Eleventh Circuit concluded that "the allegations of some Plaintiffs that they have suffered injuries resulting from *actual* identity theft support the sufficiency of all Plaintiffs' allegations that they face a *risk* of identity theft," *id.* at 1263.

Comparing Plaintiffs' allegations to these examples, *Tsao* is the closest match. Plaintiffs generally allege that they "believe their unencrypted Private Information was sold

on the dark web following the Data Breach, as that is the *modus operandi* of hackers." Am. Compl. ¶ 99; *see also id.* ¶¶ 54, 120. They do not allege that all Plaintiffs' information was *actually posted* on a particular website (nor would that necessarily be plausible if the only fact supporting the allegation is the language included in the cybersecurity notice, which is opaque as to whether the entire class's information was even *actually stolen*). The amended complaint also alleges that a single plaintiff, Edward James, Sr., suffered three instances of fraud "as a result of the Data Breach." *Id.* ¶ 153. None of these allegations is sufficient to support class-wide standing.

Neither *Tsao*, *Equifax*, nor *Green-Cooper* hold that a single conclusory allegation of misuse as to one plaintiff following a data breach is enough to supply a multi-million-member class with a universal injury based on the substantial risk of future harm. Article III requires more. And even if the cases stood for such a sweeping proposition, as I explain below, James's individual allegations suffer from deficiencies such that they cannot support his own standing, much less standing for the rest of the class.

Plaintiffs' conclusory allegation, contra Tampa General's clear implication in its cybersecurity notice, that the entire class's private information was stolen is simply implausible. *Compare id.* ¶¶ 4, 53, *with Cybersecurity Notice*. The related allegation that Plaintiffs "believe" the class's private information has been sold on the dark web is not enough either. *See* Am. Compl. ¶¶ 54, 99, 120. Without the "critical" allegation that

buttressed the complaint in *Green-Cooper* (that the entire batch of stolen data was posted for sale on a specific dark web marketplace), Plaintiffs' conclusory allegation that they believe their information has been or will be sold because that is the nature of things is speculative. *See Clapper*, 568 U.S. at 414 n.5 (explaining that an "attenuated chain of inferences" and "speculation about the unfettered choices made by independent actors not before the court" is insufficient to satisfy the "substantial risk standard" (quotations omitted)); *see also Tsao*, 986 F.3d at 1339, 1343–44 (applying *Clapper* to data breach standing).

Because the amended complaint does not plausibly plead sufficient specific misuse to establish a substantial risk of future harm, Plaintiffs' intertwined theories of injury fail.

ii. Diminished Value of Private Information

Second is Plaintiffs' suggestion that "the diminished value of [their] Private Information as a result of the Data Breach is itself a legally recognized, cognizable injury." Resp. to MTD at 8. In their view, a plaintiff's private information is "valuable property" with a "considerable market value" in both legitimate and criminal marketplaces. Am. Compl. ¶¶ 110, 115; *see also id.* ¶¶ 110–19. That value, Plaintiffs claim, "has been damaged and diminished by [the information's] compromise and unauthorized release." *Id.* ¶ 115. This argument fares no better—while lost value is a tangible injury, Plaintiffs have not shown that this injury is actual or imminent.

Although Plaintiffs allege the existence of both legal and illegal markets for the kind of information potentially compromised in the data breach, *see id.* ¶¶ 110–19, there is no allegation that any Plaintiff has (or has ever had) the intention of selling such information to data brokers, legitimate or otherwise. As should be self-evident in a suit claiming harm from a future risk of identity theft, Plaintiffs do not allege that they have sold or plan to sell their information to criminals. And the existence of a robust legal market for private information is not enough either because, "[a]t bottom, Plaintiffs' diminished-value theory assumes that the [data breach] afforded companies with whom Plaintiffs would voluntarily trade their [private information] access to [that information] without Plaintiffs' permission." *Fraga v. UKG, Inc.*, No. 22-cv-20105, 2022 WL 19486310, at *12 (S.D. Fla. May 10, 2022). "But what basis exists for that assumption? None, in the Court's estimation." *Id.* At best, the assumption is impermissible "speculation about the unfettered choices made by independent actors not before the court." *All. for Hippocratic Med.*, No. 23-235, slip op. at 10 (quoting *Clapper*, 568 U.S. at 414 n.5). Like many data breach litigants in this circuit who have unsuccessfully raised diminution of value arguments, Plaintiffs do "not adequately allege a devaluation of [their private information] . . . because [they do] not plausibly explain how the [data breach] could have harmed Plaintiffs' abilities to sell their [information]." *Fraga*, 2022 WL 19486310, at *12; *see also id.* at *10–12 (collecting cases rejecting the diminished value standing argument). "Absent any such

explanation, [the] diminished-value argument founders." *Id.* at *12; *see also In re 21st Century Oncology Customer Data Sec. Breach Litig.* (*21st Century Oncology*), 380 F. Supp. 3d 1243, 1257 (M.D. Fla. 2019) ("Plaintiffs have not alleged that their personal information has an independent monetary value that is now less than it was before the Data Breach."); *Provost v. Aptos, Inc.*, No. 17-cv-2120, 2018 WL 1465766, at *4 (N.D. Ga. Mar. 12, 2018) (finding no standing when plaintiff failed to "allege with particularity any facts explaining how her personal identity information is less valuable than it was before the Breach").

iii. Emotional Injury

Third, Plaintiffs identify the "emotional distress associated with the loss of control over their highly sensitive Private Information" as a potential intangible harm. *See, e.g.*, Am. Compl. ¶ 8; *see also* Resp. to MTD at 9. But as Plaintiffs conceded in their response to the motion to dismiss, courts in this circuit have ordinarily recognized such harms as sufficiently concrete in the data breach context only when "allegations of emotional distress" are "coupled with the substantial risk of future harm." *See* Resp. to MTD at 9 (citing *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.* (*Mednax*), 603 F. Supp. 3d 1183, 1203 (S.D. Fla. 2022)). That accords with Supreme Court precedent.

In *Lujan*, the plaintiffs claimed "esthetic" injuries arising from the extinction of endangered species. 504 U.S. at 562–63. While the Court acknowledged that aesthetic injuries are legally cognizable, the plaintiffs nevertheless lacked standing because they were not "among the injured" who might imminently lose the opportunity to observe the animals directly. *Id.* (quotation omitted); *see also id.* at 563–64 (explaining that extinction does not cause an actual or imminent injury where plaintiffs only have a vague intent to observe wildlife in the future). The same is true here. It is not enough that a plaintiff has a "special interest in the subject," emotional or aesthetic. *Id.* at 563 (cleaned up). He or she must be "directly affected." *Id.* Because Plaintiffs have not plausibly alleged a substantial risk of future identity theft under the *Tsao/Equifax/Green-Cooper* framework, their allegations of related emotional distress do not establish a concrete injury for standing purposes.

iv. Lost Benefit of the Bargain

Plaintiffs next allege that they have been tangibly injured because they lost the benefit of their bargain with Tampa General. *See* Am. Compl. ¶¶ 124, 208; Resp. to MTD at 9–10; MPA at 17–18. But they have not shown that this harm is actual.

Plaintiffs' factual allegations on this point are sparse. The primary claim is that "[w]hen agreeing to pay [Tampa General] for the provision of its health care services, Plaintiffs and other reasonable consumers understood and expected they were, in part, paying for the service and necessary data security to protect [their private information]."

Am. Compl. ¶ 124. This implied agreement was allegedly breached when Tampa General "did not provide the expected data security," resulting in Plaintiffs "receiv[ing] services that were of a lesser value than what they reasonably expected to receive under the bargains they struck." *Id.* Put differently, Tampa General "required [Plaintiffs] to provide [it] with their Private Information to receive services" and thus "impliedly promised to protect" that information "through adequate data security measures" as part of its contract with patients. *Id.* ¶¶ 227–28; *see also id.* ¶ 48.

To support this argument, Plaintiffs allege that Tampa General "made promises and representations to its Patients" that any private information collected "would be kept safe and confidential," that "the privacy of that information would be maintained," and that Tampa General "would delete any sensitive information after it was no longer required to maintain it." *Id.* ¶ 43. They also invoke Tampa General's "Privacy Practices disclosure," which states that the hospital is "required by law to maintain the privacy of your [protected health information under federal law] and to provide you with notice of our legal duties and privacy practices with respect to [that information]." *Id.* ¶ 44. The disclosure assures readers that Tampa General is "committed to protecting the privacy of your health information." *Id.* But conspicuously absent is any allegation that the named Plaintiffs (or any other class member) specifically relied on the privacy practices disclosure when deciding to become a patient. Also missing is any suggestion that the actual medical

services Plaintiffs received (tellingly there is no discussion of these services beyond the allegation that they occurred) were diminished in value by Tampa General's data security practices.

"Many courts have cast doubt on [the benefit of the bargain theory of standing in data breach litigation], especially in cases where plaintiffs do not sufficiently allege reliance on defendants' representations as to their security policies." *Mednax*, 603 F. Supp. 3d at 1205; *see, e.g.*, *21st Century Oncology*, 380 F. Supp. 3d at 1257 ("[T]here are no factual allegations demonstrating that the Parties mutually agreed that any portion of the sums paid from Plaintiffs to Defendants would be allocated to data security."). I join those courts' skepticism. Of course, "an economic injury qualifies as a concrete injury." *Debernardis v. IQ Formulations, LLC*, 942 F.3d 1076, 1084 (11th Cir. 2019). And the Eleventh Circuit has held that, in the context of a dietary supplement banned for sale by the FDA, "[a] person experiences an economic injury when, as a result of a deceptive act or an unfair practice, he is deprived of the benefit of his bargain," *id.*, by "acquir[ing] a worthless product," *id.* at 1086. But *Debernardis* was an especially narrow decision. *See id.* at 1088 ("We caution that our decision is limited to the specific facts alleged in this case—that the plaintiffs purchased dietary supplements that Congress, through the FDCA and the DSHEA, had banned from sale with the purpose of preventing consumers from ingesting an unsafe product."). The facts here are far afield from the world of FDA

regulation and "worthless" dietary supplements. While a hospital's data security practices may exert some abstract pressure on the price of healthcare services, they do not devalue the services themselves and they certainly do not render them worthless. A heart surgery is a heart surgery, data breach or not.

Because Plaintiffs have not plausibly alleged that Tampa General's data security practices deprived them of the benefit of their bargain for healthcare services, this theory of class-wide injury also fails.[5]

v. Invasion of Privacy

Fifth and finally, Plaintiffs allege that they have suffered the intangible harm of an "invasion of privacy," but that theory fails. *Id.* ¶ 208; *see also id.* ¶ 209 ("loss of privacy"). District courts in this circuit have generally declined to recognize a concrete injury based on conclusory allegations of loss of privacy in the data breach context unless those allegations are coupled with "a substantial and imminent risk of future identity theft." *See, e.g.*, *Mednax*, 603 F. Supp. 3d at 1205. As explained above, Plaintiffs have failed to plausibly plead that their information was in fact stolen and, relatedly, failed to plausibly

[5] I note, in the alternative, that even if the lost benefit of an implied bargain for data security was a freestanding cognizable injury in data breach class actions, I would still likely decline to certify a class based on such a theory of standing because it would flunk Rule 23(b)(3)'s predominance requirement. Individualized questions about Tampa General's representations, whether patients would have sought treatment elsewhere absent those representations, and whether any given patient's information was stolen, *see Cybersecurity Notice* (explaining that "some patient information" was obtained and that this information "may have included" certain pieces of information), would inevitably overwhelm common questions of law and fact. The class action device is inappropriate in such situations.

plead any such risk. Thus, Plaintiffs cannot show a class-wide injury based solely on the allegation that the data breach resulted in an invasion of privacy. Any other result would undermine *Tsao*'s conclusion that "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing." 986 F.3d at 1344.

Plaintiffs believe that their invasion-of-privacy harm suffices to establish standing under the test established by the Supreme Court in *TransUnion.* In that case, the Court explained that certain intangible harms can be concrete if they bear "a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *TransUnion*, 594 U.S. at 425 (quotations omitted); *see also* MPA at 16–17 (advancing this theory). Plaintiffs aver that the invasion of privacy tort provides the requisite "close historical or common-law analogue for their asserted injury," even though they neither bring a claim for invasion of privacy nor identify which of their claims is sufficiently akin to that common law tort. *TransUnion*, 594 U.S. at 424.

Eleventh Circuit precedent forecloses this route to standing. *Green-Cooper* reasoned "that the common-law analogue analysis is *sui generis* to legislature-made statutory violations because the Supreme Court has not applied it to any other kind of intangible harm." 73 F.4th at 890 n.9. Thus, if the cause of action in a data breach case originates from the common law, rather than from a statute, *Tsao*'s 'misuse' requirement

remains the order of the day. *Id.* Plaintiffs may not rely on *TransUnion* to rescue their common-law claims from *Tsao* and *Green-Cooper*.

In their effort to invoke *TransUnion*, Plaintiffs do not distinguish between their common-law claims and their statutory claim under the FDUTPA. And they certainly have not shown that a FDUTPA claim is analogous to the common law tort of invasion of privacy. *Cf. Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1242–50 (11th Cir. 2022) (en banc) (discussing and applying the common-law-analogue analysis at the level of a claim's individual elements); *Drazen v. Pinto*, 74 F.4th 1336, 1343 (11th Cir. 2023) (en banc) ("[T]he relationship between the harms we compare is too attenuated when a plaintiff completely fails to allege an element essential to the harm set out as a common-law comparator." (quotations omitted)). In the light of Plaintiffs' failure to identify any potential common-law analogue for their FDUTPA claim, much less a plausibly appropriate one, they have not shown standing based on *TransUnion*.[6]

[6] It is somewhat unclear whether the common-law-analogue analysis applies to state statutory claims at all. Footnote nine of *Green-Cooper* cabins the framework to "legislature-made statutory violations" but also confirms that *Tsao* remains good law after *TransUnion*. *See* 73 F.4th at 890 n.9. And although *Green-Cooper* seems to have understood *Tsao*'s application of the misuse requirement to be "in the context of a state common-law negligence claim," *see id.*, the operative complaint in *Tsao* included a statutory claim under the FDUTPA. *See Tsao*, 986 F.3d at 1336 ("Based on these alleged injuries, the Complaint claims that PDQ. . . . violated the Florida Unfair and Deceptive Trade Practices Act by failing to, among other things, maintain adequate data security practices (Count VI)." (cleaned up)); *Tsao v. Captiva MVP Rest. Partners, LLC*, No. 18-cv-1606, Compl. (Doc. 1) ¶¶ 148–60 (M.D. Fla. July 3, 2023). Because the district court decision in *Tsao* dismissed the entire complaint without prejudice for lack of standing and the Eleventh Circuit affirmed in full, applying the "misuse" requirement for standing in data breach cases to a state statutory claim was likely necessary to *Tsao*'s holding.

4. James's Individualized Standing Argument

Regardless of the ability to demonstrate class-wide standing, Plaintiffs may certify a class under Eleventh Circuit precedent so long as one named plaintiff demonstrates standing for each of the class's claims and each form of requested relief. *See Green-Cooper*, 73 F.4th at 888; *TransUnion*, 594 U.S. at 431. James presents Plaintiffs' only arguable case. He alleges that he "discovered a fraudulent charge to his bank account in the amount of $2,600.70 for the purchase of a television" and suffered "two unauthorized ATM withdrawals in the amount of $400 each from his bank account" at some indeterminate time "[s]ince the data breach." Am. Compl. ¶ 153. These allegations are both tangible harms and sufficient "misuse" to provide James a concrete injury based on the risk of future identity theft under *Tsao* and *Green-Cooper*. But that does not end the standing inquiry. James must also demonstrate that his injury (or risk of future injury) is "fairly traceable to the challenged conduct of the defendant." *Spokeo*, 578 U.S. at 338.

James has not pleaded facts plausibly alleging (nor introduced evidence establishing) that the three fraudulent charges are "fairly traceable" to Tampa General's data breach. *See Green-Cooper*, 73 F.4th at 889 n.6 ("We may review both the allegations in the complaint and evidence in the record so far to determine whether the named plaintiffs in this case have established Article III standing for class certification purposes."); *see also id.* at 890–91 (concluding that two of three named plaintiffs in a data breach class

action lacked standing on traceability grounds, despite adequately alleging a class-wide concrete injury, when the record revealed that they did not visit the affected business during the "at-risk time frame"). Evaluating traceability in the context of a data breach might not always be difficult. In *Green-Cooper*, for example, the causation question was easy because "the information for all 4.5 million cards the hackers accessed in the Brinker system were found on Joker Stash." 73 F.4th at 886–87. When a batch of private information subject to a data breach is posted for sale en masse on a single dark web marketplace, traceability flows. But when the alleged injury is based on scattered instances of individualized misuse, a more nuanced inquiry necessarily applies. That inquiry reveals several critical flaws in James's allegations.

The first traceability problem relates to the scope of the data breach. James alleges that he received a letter from Tampa General explaining that "some combination of his name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at [Tampa General] used by Defendant for its business operations" was "improperly accessed and obtained by unauthorized third parties." Am. Compl. ¶ 152. On its face, this allegation appears unequivocal that at least "some" of James's information was stolen. But the cybersecurity notice, which the amended complaint reproduces in full and relies on as a primary source, promised only that Tampa

General would "mail[] notification letters to *individuals whose information may have been involved* in this event." *See Cybersecurity Notice*. James does not attach the letter directed to him, so there is no way to confirm whether the letter contains the concrete language of his allegation or the more equivocal "may have been" that Tampa General used in the cybersecurity notice. Without a clear answer, this apparent inconsistency casts doubt on whether James's information was actually taken, which in turn bears on whether the fraud James claims to have suffered is plausibly traceable to the data breach.

But even if "some" of James's information was accessed as alleged, he does not claim that any banking or other financial information related to the fraudulent claims on his bank account was stolen. That omission is notable. Instead, he recites a laundry list of potential pieces of information that may have been accessed in some combination, but never connects them with the claimed misuse of his bank account and debit cards. *See* Am. Compl. ¶ 152 (alleging only that what was stolen "comprised some combination of" James's private information related to personal identifiers and health records, but never mentioning any financial information or the like). This creates a substantive mismatch between bank and ATM fraud and the subject-matter of the data stolen in the breach. Without additional factual allegations to bridge the gap, James has not plausibly alleged how any of the potentially stolen information could fairly cause the $2,600 unauthorized charge to his bank

account or the two $400 ATM withdrawals. The requisite leaps of factual allegations and logic present serious traceability problems.

Finally, James suffers from the same hurdle that almost every data breach plaintiff will, even those who can allege misuse: It is far from clear that the three identified instances of fraud are fairly traceable to the Tampa General data breach (or indeed, to any data breach). To be sure, "traceability does not equate to proximate cause." *Garcia-Bengochea v. Carnival Cruise Corp.*, 57 F.4th 916, 927 (11th Cir. 2023). But unlike *Garcia-Bengochea*, this is not a situation where the causation inquiry is complicated by multiple actors working in a single chain of events preventing attribution to one alone. *See id.* at 926–27. The question instead is whether the alleged misuse stems from one of many parallel, independent causes, each of which could have resulted in the harm. In *Green-Cooper*, the plaintiffs avoided this problem by alleging that thieves posted the batch of stolen credit cards en masse to a single dark web marketplace, 73 F.4th at 886, thereby rendering traceability quite plausible. Plaintiffs here make no such allegations. And James merely alleges that the data breach occurred prior to the fraudulent credit card charges, which is insufficient without allegations establishing the proximity of the fraudulent charges to the date of the data breach. *See* Am. Compl. ¶ 153. It is possible that the hackers used the information inappropriately themselves. It is also possible that they sold the information directly to another for malfeasance. Or perhaps nothing has happened from

the potential exposure of information, at least not based on the episode at Tampa General. That a plaintiff can conjure hypotheticals does not mean that he has plausibly pleaded (much less proven for purposes of final judgment after class certification) traceability. In the same vein, James's alleged injuries could have resulted from a different data breach, unrelated to Tampa General, or identity theft unconnected to a data breach at all.

James's description of how carefully he otherwise protects his private information cannot immunize his faulty allegations. *See id.* ¶ 151 (alleging that "James is very careful about sharing his sensitive Private Information," that he "stores any documents containing his Private Information in a safe and secure location," and that he "has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source"). This recitation is best understood as an attempt to support a negative inference—because James is generally careful with his private information, the fraud alleged was likely not caused by some other data breach or incident. But the very existence of this case shows that locations generally understood as "safe and secure" (like hospital computer systems) can transform into risk vectors with little warning. And tellingly, James does not allege that his private information has never been compromised before or after Tampa General's data breach incident.

Together, these flaws negate a showing of traceability, even under a plausibility standard of proof. And if evidence is required, as *TransUnion* implies must be true before

I can order individualized relief in a class action, *see* 594 U.S. at 431, then the question is not even close.

* * *

Neither James, nor any other named Plaintiff, has shown individualized standing under even the most lenient standard of proof. And Plaintiffs' numerous class-wide standing theories all fail. Thus, Plaintiffs lack standing to sue in federal court, either as individuals or as class representatives. In the light of this jurisdictional defect, I must *sua sponte* remand the case to state court under 28 U.S.C. 1447(c). *See Ladies Mem'l Ass'n*, 34 F.4th at 994.

B. Even if Plaintiffs' Had Standing, the Rule 23 Analysis Would Likely Not Favor Certification

Although I do not reach the merits of Plaintiffs' motion for preliminary class certification, I briefly explain why Plaintiffs' standing problems would also likely result in an intractable predominance problem under Rule 23(b)(3), even if I was not required to *sua sponte* remand to state court.

In the light of the standing deficiencies discussed above and the Eleventh Circuit's decisions in *Cordoba* and *Green-Cooper* outlining the relationship between standing and predominance, the class as defined is unlikely to produce a scenario where "questions of law or fact common to class members" will "predominate over . . . questions affecting only individual members," specifically, the questions surrounding the standing of each class

member. *See* FED. R. CIV. P. 23(b)(3). In fact, understanding the interaction between standing and predominance only underscores the grave nature of Plaintiffs' standing deficiencies.

"Common issues of fact and law predominate if they have a direct impact on every class member's effort to establish liability and on every class member's entitlement to injunctive and monetary relief." *Cordoba*, 942 F.3d at 1274 (cleaned up). "[C]ommon issues will not predominate over individual questions if, as a practical matter, the resolution of an overarching common issue breaks down into an unmanageable variety of individual legal and factual issues." *Id.* (quotations omitted). The inquiry "requires more of a qualitative than quantitative analysis" and entails "a pragmatic assessment of the entire action and all the issues involved." *Id.* (quotations omitted).

In *Cordoba*, the Eleventh Circuit vacated a Telephone Consumer Protection Act class based on the district court's failure to appropriately consider standing problems in the predominance inquiry. *Id.* at 1272–77. Although *Cordoba* affirmed the traditional "one named plaintiff" rule and rejected "the proposition that all class members must prove their standing before a class [can] be certified," the panel concluded that "[i]n some cases, whether absent class members can establish standing may be exceedingly relevant to the class certification analysis required by [Rule 23]." *Id.* at 1273. The issue of absent class members' Article III standing "pose[d] a powerful problem under Rule 23(b)(3)'s

predominance factor," *id.*, "because at some point before it can award *any* relief, the district court will have to determine whether each member of the class has standing," *id.* at 1274. The "essential point" is just that—"at some time in the course of the litigation the district court will have to determine whether each of the absent class members has standing before they [can] be granted any relief." *Id.* at 1275. Of course, "[t]hat is an individualized issue," *id.*, and a district court must consider it in the predominance inquiry under Rule 23(b)(3).

To be clear, *Cordoba* did "not hold . . . that a court is required to ensure that the class definition does not include *any* individuals who do not have standing before certifying a class." *Id.* at 1276. But it does instruct district courts to "consider under Rule 23(b)(3) before certification whether the individualized issue of standing will predominate over the common issues in the case, when it appears that a large portion of the class does not have standing, . . . and making that determination for these members of the class will require individualized inquiries." *Id.* at 1277. As I explained above, Plaintiffs do not allege facts that plausibly state a class-wide injury. No named Plaintiff can establish individualized standing either, preventing the "one named plaintiff" rule from kicking in. As a result, even evaluated as individuals, it seems quite likely that few members of the proposed class could establish standing when all was said and done.

Sifting through millions of class members to find a few needles in the haystack would likely require the fine-grained legal and factual analyses that ordinarily prevent a

finding of predominance under Rule 23(b)(3). *See Green-Cooper*, 73 F.4th at 893 n.14 (explaining that the district court needed to "determine whether its class definitions would require individualized proof of standing, especially as to time or effort expended to mitigate the consequences of the data breach"). That is especially so when a proposed class definition is especially broad. *See* MPA at 7 (defining the proposed settlement class as "all persons in the United States who were sent notification from [Tampa General] that their Private Information was *potentially compromised* as a result of the [data breach]" (emphasis added)); *Green-Cooper*, 73 F.4th at 892–93 (rejecting the district court's predominance analysis because the class definition was overbroad and the court failed to conduct a *Cordoba* predominance analysis as to uninjured absent class members).

Thus, even if James or another named Plaintiff established standing under the one named plaintiff rule, I would likely be unable to certify a class for failure to satisfy Rule 23(b)(3).

IV. CONCLUSION

Accordingly, the following is **ORDERED:**

1. The Clerk is directed to **REMAND** this action to the Circuit Court for the Thirteenth Judicial Circuit in and for Hillsborough County, Florida, and to transmit a certified copy of this order to the clerk of that court.

2. The Clerk is further directed to **TERMINATE** any pending motions and deadlines, and to **CLOSE** this case.

ORDERED in Tampa, Florida, on June 18, 2024.

Kathryn Kimball Mizelle
United States District Judge

Appendix A

As of June 18, 2024, Tampa General's Cybersecurity Notice read as follows:

Cybersecurity Notice

Notice to Our Patients of Cybersecurity Event

Tampa General Hospital considers the health, safety, and privacy of our patients and team members a top priority. Regrettably, this notice concerns a cybersecurity event that may have involved some of that information.

What Happened?

On May 31, 2023, through our proactive monitoring tools, TGH detected unusual activity on our computer systems. We immediately took steps to contain the activity and began an investigation with the assistance of a third-party forensic firm. Fortunately, TGH's monitoring systems and experienced technology professionals effectively prevented encryption, which would have significantly interrupted the hospital's ability to provide care for patients. However, the investigation determined that an unauthorized third party accessed TGH's network and obtained certain files from its systems between May 12 and May 30, 2023.

TGH reported the event to the FBI and provided information to support its investigation of the criminal group responsible.

What Information Was Involved?

We reviewed the files involved and determined that some patient information was included. The information varied by individual, but may have included names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by TGH for its business operations. TGH's electronic medical record system was **not** involved or accessed.

What is TGH Doing?

TGH considers the health, safety and privacy of patients and team members a top priority. The hospital is continuously updating and hardening systems

to help prevent events such as this from occurring and has implemented additional defensive tools and increased monitoring.

What Can Patients Do?

TGH will be mailing notification letters to individuals whose information may have been involved in this event and is also providing individuals whose Social Security number was involved with complimentary credit monitoring and identity theft protection services. Patients are encouraged to review statements from their health insurer and healthcare providers, and to contact them immediately if they see any services they did not receive.

For More Information:

Patients with questions can call the dedicated call center at 1-833-627-2718, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time.