UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

MILES BLACK, individually and on behalf of all others similarly situated, and MELISSA BLACK, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

IEC GROUP, INC, d/b/a Ameriben,

Defendant.

Case No. 1:23-cv-00384-AKB

MEMORANDUM DECISION AND ORDER RE DEFENDANT'S MOTION TO DISMISS

Pending before the Court is Defendant IEC Group, Inc., d/b/a Ameriben's Motion to Dismiss Plaintiffs' Class Action Complaint (Dkt. 24). The Court finds oral argument would not significantly aid its decision-making process and decides the motion on the parties' briefing. Dist. Idaho Loc. Civ. R. 7.1(d)(1)(B); *see also* Fed. R. Civ. P. 78(b) ("By rule or order, the court may provide for submitting and determining motions on briefs, without oral hearings."). For the reasons discussed, the Court grants Ameriben's motion to dismiss.

I. BACKGROUND

Ameriben contracts with employers to provide health insurance administration services. (Dkt. 1 at ¶¶ 9, 21-22). Plaintiffs Miles Black and Melissa Black received health insurance benefits from a plan that Ameriben administered. (*Id.* at ¶¶ 22-24). In August 2023, Ameriben notified the Blacks that certain information related to them was part of a data breach. (*Id.* at ¶¶ 12, 26). The breach occurred in December 2022 when an Ameriben employee emailed a spreadsheet containing

"a claims report" to "one or more members." (*Id.* at ¶ 25; Dkt. 1-3 at p. 2). The spreadsheet was filtered to show only the recipient's personal information. (Dkt. 1-3 at p. 2).

In July 2023, however, Ameriben discovered the spreadsheet could possibly be unfiltered to display the personal information of other members, including the Blacks. (Dkt. 1 at ¶¶ 12, 25; *see* Dkt. 1-3 at pp. 2-7). On August 14, 2023, Ameriben sent a letter to each of the Blacks notifying them of the potential disclosure of their information, explaining how to protect their identity, and advising them of their right to receive one or more free credit reports from each of the major credit reporting bureaus. (Dkt. 1-3 at p. 3). Further, Ameriben explained the personal information potentially disclosed included the Blacks' "first and last name, the employee's first and last name (if someone other than [the Blacks]), a unique tracking ('cert') number, provider name, claim number, date of service, and the amount billed or paid." (Dkt. 1-3 at p. 2).

Approximately ten days later, on August 25, 2023, the Blacks filed this lawsuit on behalf of themselves and a putative class of similarly situated individuals. (Dkt. 1 at ¶ 7). They allege Ameriben failed "to properly secure and safeguard customers' sensitive personally identifiable information" including "their names, sensitive financial information, and protected health information" such as "customers' member[] identification numbers, healthcare provider, and health insurance information." (Dkt. 1 at ¶ 7). Based on this disclosure of information, the Blacks allege numerous claims for relief including negligence, negligence per se, breach of contract, breach of implied contract, breach of fiduciary duty, unjust enrichment/quasi contract, and violation of Florida statutory law. (Dkt. 1 at ¶¶ 118-214).

The Blacks identify principally five categories of injuries, most of which relate to a risk of future identity theft or fraud and include: (1) the unauthorized use or misuse of their information (Dkt. 1 at ¶ 82 a, b, c); (2) mitigation costs and lost time associated with protecting their

information (*id.* at ¶ 82 d, e, h); (3) the "continued risk" their information is subject to further breaches by Ameriben (*id.* at ¶ 82 g); (4) "[t]he imminent and certain impending injury flowing from potential fraud and identity theft" (*id.* at ¶ 82 f); and (5) "fear, anxiety, and stress." (*Id.* at ¶¶ 91, 103). They seek declaratory and injunctive relief and damages. (Dkt. 1 at p. 49, ¶¶ B, C, D). In response, Ameriben filed a motion to dismiss under Rule 12(b)(1) and (b)(6) of the Federal Rules of Civil Procedure, arguing the Blacks lack standing and fail to state a claim for relief. (Dkt. 24).

II. LEGAL STANDARD

A motion to dismiss under Rule 12(b)(1) challenges the Court's subject matter jurisdiction. The plaintiff bears the burden of establishing subject matter jurisdiction exists. *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). A motion to dismiss for lack of standing is properly brought under Rule 12(b)(1) because standing is a jurisdictional matter. Fed. R. Civ. P. 12(b)(1). A jurisdictional challenge may be facial or factual. *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). "A 'facial' attack accepts the truth of the plaintiff's allegations but asserts that they are insufficient on their face to invoke federal jurisdiction." *Id.* "A 'factual' attack, by contrast, contests the truth of the plaintiff's factual allegations, usually by introducing evidence outside the pleadings." *Id.*

III. ANALYSIS

A. Standing

Ameriben facially challenges the Blacks' standing to assert their claims. (Dkt. 24-1 at pp. 4-8). Article III of the United States Constitution limits the scope of federal judicial power to the adjudication of cases and controversies. U.S. Const. art. III, § 2. A fundamental safeguard of that constitutional limitation is the doctrine of standing. *See Lujan v. Defenders of Wildlife*, 504

U.S. 555, 560 (1992); *see also E. Bay Sanctuary Covenant v. Trump*, 932 F.3d 742, 765 (9th Cir. 2018). "The Article III standing inquiry serves a single purpose: to maintain the limited role of courts by ensuring they protect against only concrete, non-speculative injuries." *E. Bay Sanctuary Covenant v. Biden*, 993 F.3d 640, 662 (9th Cir. 2021) (citing *Lujan*, 504 U.S. at 583). "Whether a plaintiff has standing (and thus, whether the court has jurisdiction) is a threshold question that is distinct from the merits of [the] claim." *Sabra v. Maricopa Cnty. Cmty. Coll. Dist.*, 44 F.4th 867, 878-79 (9th Cir. 2022) (internal quotation marks omitted).

Plaintiffs bear the burden to show standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016), *as revised* (May 24, 2016). At least one named plaintiff must have standing in a class action. *Frank v. Gaos*, 586 U.S. 485, 492 (2019). Further, "plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). To satisfy Article III's standing requirement, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *Id.* at 423. "To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo*, 578 U.S. at 339 (internal quotation marks omitted).

1. Risk of Future Harm as Injury-in-Fact

Ameriben's challenge to the Blacks' Article III standing focuses on the first element and asserts the Blacks have failed to allege an imminent injury-in-fact. (Dkt. 24-1 at p. 4). The Ninth Circuit has at least twice addressed whether a disclosure of personal information presents an imminent and credible risk of harm for purposes of satisfying the injury-in-fact requirement for

standing. In *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010), plaintiffs brought a putative class action against Starbucks for negligence and breach of contract after a laptop containing the names, addresses, and social security numbers of approximately 97,000 former Starbucks employees was stolen. One plaintiff alleged she had been "extra vigilant" about and spent a "'substantial amount of time'" watching her financial accounts and planned to pay to have her credit monitored in the future. *Id.* at 1141. Another plaintiff alleged spending "substantial amounts of time" checking his financial accounts, placed fraud alerts on his credit cards, and had "generalized anxiety and stress regarding the situation." *Id.* A third plaintiff alleged someone attempted to open a bank account using his social security number but no financial loss resulted. *Id.*

In addressing whether plaintiffs had sufficiently alleged an injury-in-fact for purposes of standing, the Ninth Circuit in *Krottner* noted the only alleged "present" injury was one plaintiff's alleged anxiety and stress; the plaintiffs' "remaining allegations concern[ed] their increased risk of future identity theft." *Id.* at 1142. Regarding this risk of future harm, the Ninth Circuit ruled that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Id.* at 1143 (quoting *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007)). Accordingly, the Ninth Circuit ruled that "because the plaintiffs had alleged an act that increased their risk of future harm, they had alleged an injury-in-fact sufficient to confer standing." *Id.*

Subsequently, the Ninth Circuit in *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018), addressed standing in an analogous context and considered whether *Krottner* remains good law

after the Supreme Court's decision in *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).[1] In *Zappos.com*, hackers targeted the servers of Zappos, a retailer, and stole the personal information of more than 24 million Zappos customers, including their "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information." *Zappos.com*, 888 F.3d at 1023. Concluding *Krottner* remained good law, the Ninth Circuit in *Zappos.com* noted that "the sensitivity of the personal information, *combined with its theft*, led [it] to conclude that the plaintiffs had adequately alleged an injury in fact in standing" in *Krottner*. *Zappos.com*, 888 F.3d at 1027 (emphasis added). In other words, the Court in *Zappos.com* considered both the nature of the sensitive information and the context in which it was disclosed, i.e, by theft. Based on *Krottner*, the Ninth Circuit concluded in *Zappos.com* that the plaintiffs had alleged the theft of the type of information, including their credit card information, which could be used to commit identity theft and that, as a result, the plaintiffs had alleged an injury-in-fact. *Id.*

Since the Ninth Circuit's decisions in *Krottner* and *Zappos.com*, the Supreme Court has addressed the requisite showing of an injury-in-fact for establishing standing in *TransUnion*. In that case, a class of 8,185 individuals sued TransUnion, claiming it "failed to use reasonable procedures to ensure the accuracy of their credit files." *Id.* at 417. The Court explained that in determining "the concrete-harm requirement" for standing, "courts should assess whether the alleged injury to the plaintiff has a 'close relationship' to harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 424.

---

[1] In *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 401 (2013), the Supreme Court ruled that plaintiffs' allegations that "there [was] an objectively reasonably likelihood that their [private, confidential] communications would be acquired under [50 U.S.C. § 1881a of the Foreign Intelligence Surveillance Act of 1978] at some point in the future" was "too speculative" to satisfy the requirement that an injury-in-fact be "certainly impending" for purposes of injunctive relief.

Considering whether those class members whose credit files were *not* provided to third parties had standing, the *TransUnion* Court concluded they did not. *Id.* at 437. It ruled those "plaintiffs did not demonstrate that the risk of future harm materialized," i.e., they did not establish TransUnion had ever provided inaccurate information to third parties. *Id.* Further, the Court ruled the risk of future harm of dissemination to third parties was too speculative to support Article III standing for their damage claims. *Id.* at 438.

Since the Supreme Court's decision in *TransUnion*, at least two district courts in the Ninth Circuit have questioned *Krottner* and *Zappos.com* as inconsistent with *TransUnion*. For example, one district court ruled the theory that "the threat of identity theft posed by a data breach, without more, can constitute an injury-in-fact[] is no longer viable" under *TransUnion*. *Leonard v. McMenamins, Inc.*, No. 2:22-CV-00094-BJR, 2022 WL 4017674, at *2 (W.D. Wash. Sept. 2, 2022). Another noted that "in light of *TransUnion*'s rejection of risk of harm as a basis for standing for damages claims, the Court questions the viability of *Krottner* and *Zappos.com*'s holdings finding standing on this very basis." *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1054 n.15 (N.D. Cal. 2022); *cf. Bock v. Washington*, 33 F.4th 1139, 1145 (9th Cir. 2022) (citing *TransUnion* and noting "the Supreme Court is clear that where a risk of future harm has not yet materialized, the plaintiffs' argument for standing for their damages claims based on an asserted risk of future harm is unavailing").

Nevertheless, the Blacks rely on *Krottner* and assert they have standing because Ameriben's disclosure of personal information allegedly creates a substantial risk of future identity theft and fraud. (*See* Dkt. 24-1 at pp. 4-8; *see also* Dkt. 1 at ¶ 82, a, b, c, f, g (alleging information is subject to potential fraud and identity theft, misuse, and continued risk of further breaches)). Even assuming the rulings in *Krottner* and *Zappos.com* remain good law despite the Supreme

Court's subsequent ruling in *TransUnion* that allegations of a future risk of harm are inadequate to establish standing to seek damages, the Blacks' allegations of future harm are insufficient to demonstrate standing under *Krottner* and *Zappos.com* for at least two reasons.

a. Nature of Information Disclosed

First, the nature of the information Ameriben allegedly disclosed does not give rise to a credible threat of fraud or identity theft. "The Ninth Circuit identifies types of future harm in data breach cases based on the types of personal information compromised." *Greenstein v. Noblr Reciprocal Exchange*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022). "[I]n data breach cases, courts must examine the nature of the specific information at issue to determine whether privacy interests were implicated at all. Otherwise, every data breach . . . would confer standing, regardless of whether private information is exposed." *Zynga*, 600 F. Supp. 3d at 1050. Such an examination is consistent with requiring a plaintiff to demonstrate concrete injury to "ensure[] that federal courts decide only the rights of individuals and that federal courts exercise their proper function in a limited and separated government." *TransUnion*, 594 U.S. at 423 (internal citations and quotation marks omitted).

Considering the type of personal information Ameriben allegedly disclosed in this case, there is no cognizable, imminent threat of future harm to the Blacks. Some of the information Ameriben disclosed is not private, including the Blacks' names (or those of others related to them). Although Ameriben's disclosure of certain health-related information may be considered private, this information is not the type of information hackers generally rely on to steal identity or to access financial resources. *See Greenstein*, 585 F. Supp. 3d at 1227 (noting "driver's license numbers do not provide hackers with a clear ability to commit fraud and are considered not as sensitive as social security numbers").

Moreover, the information Ameriben disclosed does not involve "matters of a kind that would be highly offensive to a reasonable person" necessary to assert a privacy claim. *Zynga*, 600 F. Supp. 3d at 1049 (internal quotation marks omitted); *see also TransUnion*, 594 U.S. at 424 (requiring alleged injury to bear close relationship to traditionally recognized harm); *Uranga v. Federated Publications, Inc.*, 67 P.3d 29, 32-33 (Idaho 2003) (discussing standard for invasion of privacy by intrusion and for disclosure of private facts). While disclosure of private information can present a concrete injury, the Court rejects the assertion that the information disclosed here is of the type that would be highly offensive to a reasonable person.

Further, although the Blacks alleged Ameriben disclosed their "sensitive financial information," Blacks' allegations acknowledge that information related only to "the amount billed or paid." (*Compare* Dkt. 1 at ¶ 7 (describing disclosed information as "sensitive financial information") *with id.* at ¶ 12 (acknowledging alleged sensitive information was "the amount billed or paid); *see also* Dkt. 1-3 (notifying Blacks the disclosed information included "amount billed or paid")). The disclosure of amounts billed or paid is substantially different than the disclosure of credit or debit card information, which provides a thief with an avenue to readily access financial resources. Further, the Blacks fail to allege or explain how disclosure of the amounts billed and paid subjects them to an increased risk of identity theft or fraud. Rather, they acknowledge the information is not the type that is "tempting" or "most valuable to hackers." (Dkt. 1 at ¶ 35).

Accordingly, the Court finds the information Ameriben allegedly disclosed is not sufficiently sensitive to give hackers the means to commit fraud or identity theft. *See Zappos.com*, 888 F.3d at 1027 (holding injury in fact exists where information obtained from data breach is "sufficiently sensitive" to "g[ive] hackers the means to commit fraud or identity theft"); *Patterson v. Med. Rev. Inst. of Am.*, LLC, No. 22-CV-00413-MMC, 2022 WL 2267673, at *2 (N.D. Cal.

June 23, 2022) (ruling disclosure of name, medical information, and amount billed, among other information, was inadequate to create risk of fraud or identity theft); *Greenstein*, 585 F. Supp. 3d at 1228-29 (finding no "credible threat of future" identity theft where data breach did not involve "social security or credit card information" or other information that could be used to "open a new account in [p]laintiffs' names or to gain access to personal accounts likely to have more sensitive information"); *Antman v. Uber Techs., Inc*., Case No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (holding no "credible risk of identity theft" exists "[w]ithout a hack of information such as social security numbers, account numbers, or credit card numbers").

2. Context of Disclosure

Second, the context in which Ameriben's data breach occurred makes it unlikely the Blacks' information will be stolen and misused. Generally, courts avoid "rel[ying] on a highly attenuated chain of possibilities" to find a risk of harm substantial and imminent. *Clapper*, 568 U.S. at 410. Relatedly, plaintiffs cannot rely on speculation about the unfettered choices made by independent actors not before the court to allege a substantial risk of harm. *Id.* at 414 n.5; *see also Beck v. McDonald*, 848 F.3d 262, 273-74 (4th Cir. 2017) (finding plaintiffs' failure to allege "the data thief intentionally targeted the personal information" rendered risk of future identity theft too speculative); *Dearing v. Magellan Health Inc.*, No. CV-20-00747-PHX-SPL, 2020 WL 7041059, at *2 (D. Ariz. Sept. 3, 2020) (ruling risk not substantial or certainly impending where plaintiffs' information was not "deliberately targeted" or "even stolen").

The Blacks acknowledge that the data breach was the result of an Ameriben employee sending a filtered spreadsheet to one or more members and that someone must "unfilter" the spreadsheet to access the Blacks' information. (Dkt. 1 at ¶ 25). This circumstance is different than in *Krottner* and *Zappos.com* where the data breach occurred due to a theft of the information

versus, as in this case, an inadvertent disclosure of information. Absent nefarious conduct causing the data breach, it is speculative someone may misuse the Blacks' information in the future. Because neither the nature of the information Ameriben disclosed nor the context in which Ameriben disclosed it establish the Blacks are subject to an imminent risk of harm that is not conjectural or hypothetical, they have failed to allege injury-in-fact for standing.

3. Other Alleged Injuries

Absent a credible risk of fraud or identity theft, the Blacks' other alleged injuries—including their mitigation costs and their fear, anxiety, and stress—fail to establish an injury-in-fact for purposes of standing. Courts have routinely rejected these types of injuries as establishing an injury-in-fact, reasoning that a plaintiff cannot manufacture standing based on a hypothetical future harm. *Clapper*, 568 U.S. at 416 (ruling plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"); *Antman*, 2015 WL 6123054, at *11 (ruling "mitigation expenses do not qualify as injury; the risk of identity theft must first be real and imminent, and not speculative, before mitigation costs establish injury in fact"); *Greenstein*, 585 F. Supp. 3d at 1230 (ruling plaintiffs' efforts and costs attempting to mitigate harm does not confer standing); *Patterson*, 2022 WL 2267673, at *2 (ruling plaintiff cannot "manufacture standing by inflicting harm on [himself] based on [his] fear of *hypothetical* future harm that is not certainly impending"); *Callahan v. Ancestry.com, Inc.*, No. 20-cv-08437-LB, 2021 WL 2433893, at *4-5 (N.D. Cal. June 15, 2021) (holding, in data breach context, "anxiety and stress" without "credible threat of future identity theft" is not cognizable injury in fact); *Antman*, 2015 WL 6123054, at *11 (holding risk of identity theft must first be real and imminent before mitigation costs establish injury-in-fact).

Finally, the Blacks' receipt of spam texts, calls, and emails and their time spent "sifting through" this unwanted information does not constitute injury-in-fact for standing. (Dkt. 33 at p. 16). Courts generally reject that a plaintiff's receipt of spam messages is an injury sufficient to confer standing. *See Zynga*, 600 F. Supp. 3d at 1051 (citing cases); *Jackson v. Loews Hotels, Inc.*, No. ED CV 18-827-DMG, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (citing cases). Moreover, absent allegations that Ameriben disclosed the Blacks' email addresses or their telephone numbers, that the Blacks' receipt of spam relates to Ameriben's data breach is speculative. *See Lujan*, 504 U.S. at 560 (ruling injury must be traceable to defendant's conduct). Accordingly, the Blacks' other alleged injuries fail to establish standing for either injunctive relief or damages.

IV. CONCLUSION

The Court concludes the Blacks lack standing to assert their claims for damages and for injunctive and declaratory relief. Because the Court lacks subject matter jurisdiction, it does not address Ameriben's alternative arguments in support of its motion for dismissal under Rule 12(b)(6). The Blacks, however, should carefully consider the viability of those arguments if they amend their complaint.

V. ORDER

IT IS ORDERED that:

1. Defendant's Motion to Dismiss Plaintiffs' Class Action Complaint (Dkt. 24) is **GRANTED** without prejudice.

2. Plaintiffs are **GRANTED** leave to file an amended complaint to cure the deficiencies identified in this order. *See Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052

(9th Cir. 2003) (providing dismissal without leave to amend is not appropriate unless clear complaint cannot be saved by amendment). If Plaintiffs choose to file an amended complaint, they must file that complaint within twenty-one (21) days of this order's entry unless an extension is granted for good cause shown.

DATED: July 30, 2024

Amanda K. Brailsford
U.S. District Court Judge