

**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**

**I.C., ET AL.,**

Plaintiffs,

vs.

**ZYNGA, INC.,**

Defendant.

CASE NO. 20-cv-01539-YGR

**ORDER GRANTING MOTION TO DISMISS**

Re: Dkt. No. 96

Plaintiffs bring this consolidated putative class action against social gaming company Zynga Inc. in connection with a large-scale data breach of players' account information. The Court previously granted Zynga's motion to dismiss the first consolidated class action complaint for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(1), permitting plaintiffs to amend their pleadings. Currently pending is Zynga's motion to dismiss the second consolidated class action complaint ("SAC") on the same basis. (Dkt. No. 96.) Having carefully reviewed the pleadings and the briefing on the motion, and for the reasons stated below, the Court hereby **GRANTS** the motion **WITHOUT LEAVE TO AMEND**.<sup>1</sup>

**I. BACKGROUND**

The SAC (Dkt. No. 95) alleges as follows:

Zynga develops, markets, and operates live social games including the popular *Words With Friends* and *Farmville* franchises. (SAC ¶ 42.) These games are played on the Internet, social networking sites, and mobile platforms "by millions of people around the world each day." (*Id.*) Plaintiffs were among such players. (*Id.* ¶¶ 8–37.) Zynga offers a mix of paid and free games to players while also providing advertising services to advertising agencies and brokers. (*Id.* ¶¶ 42, 44.) The free games are supported by in-game advertisements, in-game purchases, and Zynga's collection and sale of users' personal identifying information ("PII"). (*Id.* ¶ 44.)

One must create an account with Zynga to play its games. (*Id.* ¶ 47.) "In connection with

---

<sup>1</sup> Pursuant to Federal Rule of Civil Procedure 78(b) and Civil Rule 7-1(b), the Court finds this motion appropriate for decision without oral argument.

1 the account creation process, Zynga collects certain PII from users, including their first name, last  
 2 name, email address, gender, and a password for the account, if one was created.” (*Id.* ¶ 48.)  
 3 Users “have the option to link their Zynga account to their Facebook account instead of providing  
 4 an email address. If a prospective user chooses to log in with Facebook, the prospective user must  
 5 provide their Facebook username and/or phone number and password through a separate  
 6 authentication screen.” (*Id.* ¶ 49.) The SAC further alleges, “[u]pon information and belief,  
 7 before it began using a third-party payment processor, Zynga collected financial information, such  
 8 as credit card details, for game purchases or in-app purchases.” (*Id.* ¶ 50.)

9 On September 12, 2019, Zynga posted on its website the following statement, titled  
 10 “Player Security Announcement,” which stated in relevant part:

11  
 12 We recently discovered that certain player account information may have been  
 13 illegally accessed by outside hackers. An investigation was immediately  
 14 commenced, leading third-party forensics firms were retained to assist, and we  
 15 have contacted law enforcement.

16 While the investigation is ongoing, we do not believe any financial information  
 17 was accessed. However, we have identified account login information for certain  
 18 players of *Draw Something* and *Words With Friends* that may have been  
 19 accessed. As a precaution, we have taken steps to protect these users’ accounts  
 20 from invalid logins. We plan to further notify players as the investigation  
 21 proceeds.

22 (*Id.* ¶ 84.) Zynga “never notified those customers by email, or even by a pop-up notification”  
 23 regarding the data breach or “offer[ed] any assistance with mitigating the risks associated with  
 24 same.” (*Id.* ¶¶ 12, 86.)

25 On September 29, 2019, The Hacker News reported that a serial hacker breached Zynga’s  
 26 customer database and acquired the information of more than 218 million users. (*Id.* ¶ 67.) The  
 27 hacker reported that the breach affected all Android and iOS game players who had installed and  
 28 signed up for the *Words With Friends* game on or before September 2, 2019. (*Id.*) The SAC  
 alleges that the affected users’ PII have been sold or otherwise published on the dark web. (*Id.* ¶  
 114.)

According to the SAC, identity theft can occur by using the PII stolen from Zynga. (*Id.* ¶

1 95.) For example, a cyber attacker can take “a massive trove of usernames and passwords from a  
2 data breach and tr[y] to ‘stuff’ those credentials into the login page of other digital services.” (*Id.*  
3 ¶ 97.) “The vast majority of email and password comb[inations] [will not] work, but a few will.  
4 That[ is] because many people reuse the same credentials on multiple websites.” (*Id.* ¶ 103  
5 (internal quotation marks and citation omitted).) In addition to these so-called credential stuffing  
6 attacks, the breached data includes “enough information for hackers to potentially create targeted  
7 phishing attacks made up to look as if they are an official communication from Zynga.” (*Id.* ¶ 101  
8 (internal quotation marks and citation omitted).) “The communications can also look like they are  
9 from other trusted companies, such as banks, and claim that there is suspicious activity on the  
10 account to tempt a person to click on a link and provide additional valuable PII.” (*Id.* (citation  
11 omitted).) The information stolen from Zynga is “highly valued amongst cyber thieves and  
12 criminals,” creating a “well-established market” on the dark web. (*Id.* ¶ 96.) The SAC cites a  
13 number of reports describing the financial, emotional, and physical injuries that victims of identity  
14 theft can suffer, particularly for minors, who comprise “a substantial portion of [Zynga’s] user  
15 base.” (*Id.* ¶¶ 59–64, 131–38.)

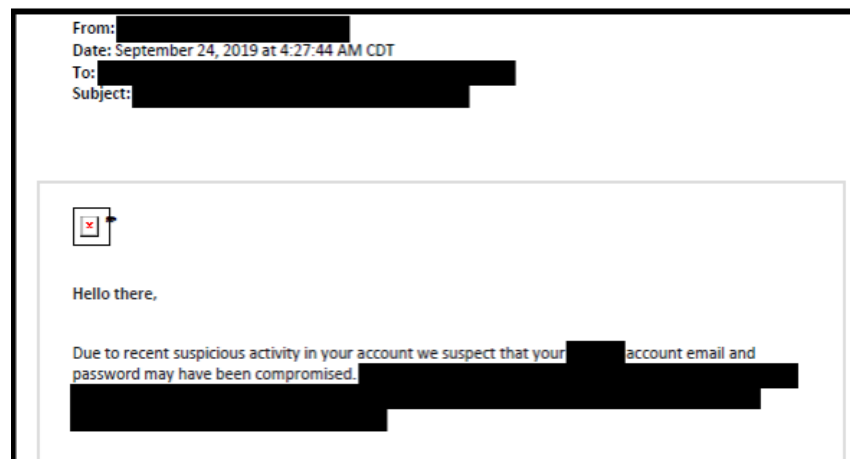
16 The SAC is not entirely consistent regarding the information stolen in the breach. At  
17 minimum, the information allegedly stolen included names, email addresses, phone numbers,  
18 Zynga usernames, Zynga passwords (some hashed and some in plain text), Zynga password reset  
19 tokens, and Facebook usernames. (*Id.* ¶ 67.) The SAC includes gender, home address, and credit  
20 card information in the definition of “PII” but does not specifically allege that this data was taken  
21 in the breach. (*Compare id.* ¶ 2 n.1 *with id.* ¶ 67.) The SAC also alleges that the stolen  
22 information included “dates/times when the account was created, last accessed, and the IP address  
23 of the last login,” but did not include such information in the PII definition. (*Compare id.* ¶ 67  
24 *with id.* ¶ 2 n.1.) In addition, the SAC alleges both that users’ dates of birth were stolen but also  
25 that Zynga did not collect information regarding a user’s age or date of birth. (*Compare id.* ¶ 2 n.1  
26 *with id.* ¶ 48.) Further, while alleging that Facebook passwords were stolen, the SAC also alleges  
27 that Zynga reportedly does not collect Facebook passwords and that the hacker only claimed to  
28 have accessed “the ‘Facebook IDs’ of Zynga users.” (*Compare id.* ¶ 2 n.1 *with id.* ¶ 68.)

1 Named plaintiffs are Zynga players whose information was allegedly hacked during the  
 2 breach: I.C., Amy Gitre, Carol Johnson, Lisa Thomas, Joseph Martinez IV, Daniel Petro, and  
 3 Christopher Rosiak. (*Id.* ¶¶ 8, 14, 16, 23, 25, 27, 31.) The Court previously granted Zynga’s  
 4 motion to compel arbitration of the claims of Gitre, Thomas, and Martinez. (Dkt. No. 93.) With  
 5 respect to the remaining plaintiffs, the following information was allegedly stolen:

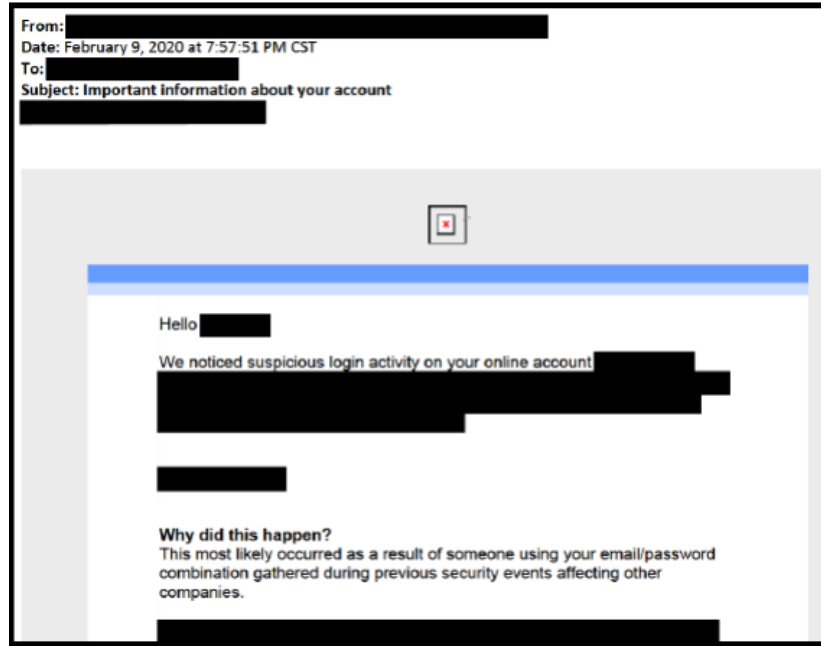
- 6 • Petro: email address and Zynga username
- 7 • I.C.: email address, Zynga username, and Zynga password
- 8 • Johnson: email address, Zynga username, *Games with Friends* hashed  
 9 password, *Draw Something* plain text password, date of birth,  
 10 phone number, and Zynga password reset tokens
- 11 • Rosiak: email address, Zynga username, Zynga password, phone number,  
 12 Facebook name, and Facebook username

13 (*Id.* ¶¶ 10, 19, 30, 31.) The only plaintiff that allegedly had their Zynga password stolen in plain  
 14 text form is Johnson. (*Id.* ¶¶ 19, 74.) Zynga did not directly notify these plaintiffs that their  
 15 information had been compromised by the breach. (*Id.* ¶¶ 8, 17, 29, 34.) I.C., Johnson, and Petro  
 16 confirmed through the website haveibeenpwned.com, and Rosiak received notices from an identity  
 17 theft monitoring service, about the same. (*Id.* ¶¶ 8, 17, 29, 34–35, 120–121.)

18 In the aftermath of the data breach, each of the named plaintiffs allege they were affected  
 19 by the breach in a number of ways. I.C., who is a minor, received at least three notices regarding  
 20 non-Zynga accounts indicating that I.C.’s login information may be compromised, reproduced  
 21 below.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

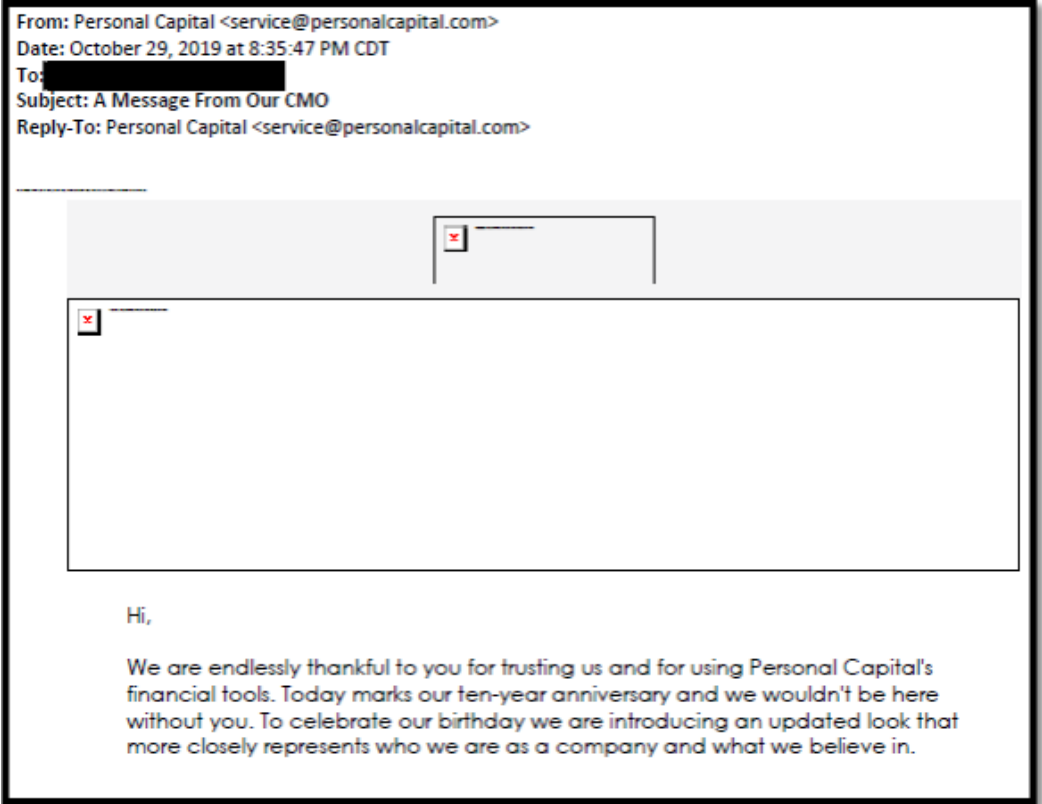


(*Id.* ¶¶ 106, 109, 112.) Two of those notices concerned other gaming accounts.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

I.C. also received at least two suspicious emails, including one from Personal Capital, reproduced below.

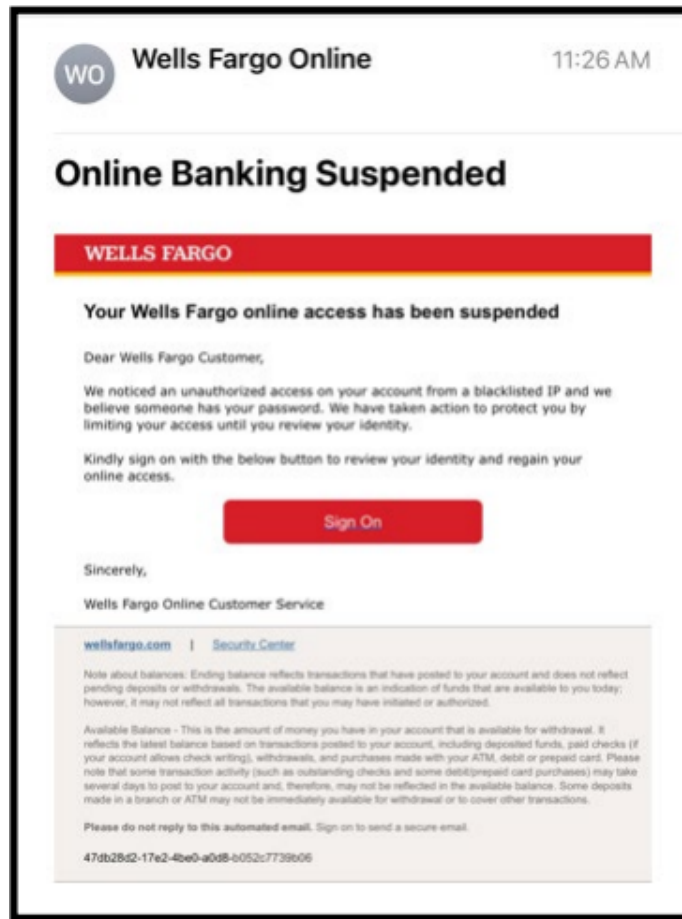
From: Mary <[REDACTED]>  
Date: November 16, 2019 at 4:31:02 PM CST  
To: "[REDACTED]" <[REDACTED]>  
Subject: Re: [REDACTED]  
  
Evening  
is it [REDACTED]?



(*Id.* ¶¶ 107, 111.) I.C. has no knowledge or experience with Personal Capital, which markets itself as an online financial advisor and personal wealth management company. (*Id.* ¶ 111.) I.C. “used his Zynga password for approximately 90% of his online accounts, including email, entertainment, gaming, social media popular with youth, and others.” (*Id.* ¶ 105.) After learning of the data breach in January 2020, I.C. “spent hours attempting to update his account passwords”

1 and “install[ing] a two-factor authentication application” but could not be certain that he did so for  
2 all of his accounts. (*Id.* ¶¶ 116–18.)

3 Rosiak was “inundated” with suspicious email, calls and texts. (*Id.* ¶¶ 125, 129.) One  
4 such text was addressed to “Henry,” which is the first name of his fake Facebook account. (*Id.* ¶  
5 129.) He also received an email purportedly from Wells Fargo, reproduced below, that was  
6 “likely a phishing email.”



23 (*Id.* ¶ 128.) Rosiak never had a Wells Fargo banking account. (*Id.*) In addition, he received  
24 Facebook “friend suggestions” and “people you may know” from individuals, none of whom he  
25 knew or had any connection. (*Id.* ¶ 126.)<sup>2</sup> Rosiak “spent considerable time changing all of his  
26

27  
28

---

<sup>2</sup> The SAC includes the screenshots of these individuals as well as their names (Mirazad Mirazad, UMii Aiman, Ubb Ibaid, Riya Mandal, Awara Ladka, B Hat Zurjn, MaHi INhu, and Eshutosh Paikra) and notes that the hacker is from Pakistan. (Compl. ¶ 126.) The Court declines to speculate as to what inference plaintiffs are attempting to draw.

1 passwords,” deleted his Facebook account, changed his voice mail message to a generic message  
2 that did not reveal his first name, and experienced “considerable alarm, stress and concern.” (*Id.*  
3 ¶¶ 125, 127, 129, 130.)

4 Johnson, who is a septuagenarian and “not particularly computer-savvy,” experienced an  
5 increase in phishing emails. (*Id.* ¶¶ 20, 21.) She also “used the same password she provided to  
6 Zynga for many other online accounts, including her email account which she uses to send  
7 confidential information such as financial information and communications with her doctor’s  
8 office.” (*Id.* ¶ 20.) Johnson “spent at least three to four hours in an attempt to mitigate . . . against  
9 the risk of identity theft and fraud upon learning the Zynga data breach.” (*Id.*) She and her sister  
10 “went through every online account she could think of that had the same password as her Zynga  
11 account in an attempt to change the passwords.” (*Id.*) The foregoing has caused her “considerable  
12 alarm, stress, and concern.” (*Id.* ¶ 22.)

13 Petro received Facebook friend requests from individuals with whom he had no  
14 connection. (*Id.* ¶ 30.) He also received multiple spam and robo calls on the phone he uses to  
15 access his Zynga account. (*Id.*)

16 Beginning in March 2020, plaintiffs individually filed putative class actions against Zynga  
17 in connection with the September 2019 data breach. Zynga filed motions to compel arbitration in  
18 three of the four actions based on the mandatory arbitration provision in the applicable terms of  
19 service. Because it was unclear which terms plaintiffs accepted, the Court denied the motions but  
20 directed plaintiffs to provide their contact information to enable Zynga to review plaintiffs’ Zynga  
21 accounts. (Dkt. No. 60.) After consolidation of the actions, plaintiffs filed a consolidated class  
22 action complaint. (Dkt. No. 67.) Thereafter, Zynga filed a renewed motion to compel arbitration  
23 as well as a motion to dismiss the FAC for lack of subject matter jurisdiction under Rule 12(b)(1)  
24 and for failure to state a claim under Rule 12(b)(6). (Dkt. Nos. 71, 72.) Upon hearing arguments,  
25 the Court granted the motion to compel as to Gitre, Thomas, and Martinez, as well as the motion  
26 to dismiss. (Dkt. No. 93.) The Court permitted plaintiffs to file an amended complaint and  
27 permitted defendants, should they again move to dismiss under Rule 12(b)(1), to defer any Rule  
28 12(b)(6) challenges.



1           The SAC alleges 29 causes of action under state common and statutory law, some of which  
2 are asserted in pairs (respectively brought by the minor plaintiff and the other plaintiffs):  
3 negligence (counts I and II); negligence per se (counts III and IV); negligent misrepresentation  
4 (counts V and VI); breach of contract (counts VII and counts VIII); unjust enrichment (counts IX  
5 and X); breach of confidence (count XI); violation of state data breach statutes (counts XII and  
6 XIII); intrusion upon seclusion (counts XIV and XV); declaratory judgment (counts XVI and  
7 XVII); violations of California Unfair Competition La (count XVIII), California False Advertising  
8 Law (count XIX), California Consumers Legal Remedies Act (count XX), Missouri  
9 Merchandising Practices Act (count XXI), Wisconsin Deceptive Trade Practices Act (count  
10 XXII), Colorado Consumer Protection Act (count XXIII), Iowa Consumer Fraud Act (count  
11 XXIV), Indiana Deceptive Consumer Sales Act (count XXV), Kansas Consumer Protection Act  
12 (count XXVI), and Michigan Consumer Protection Act (XXVII); and publicity given to private  
13 life (counts XXVIII and XXIX). The SAC alleges that Zynga failed to protect its customers' PII  
14 by, among other things, using outdated password encryption methods that were banned for use by  
15 federal government agencies as early as 2010. (SAC ¶ 3.)

16           Zynga now moves to dismiss the SAC for lack of subject matter jurisdiction under Rule  
17 12(b)(1). Specifically, Zynga contends that plaintiffs fail to allege a concrete injury in fact such  
18 that they cannot establish Article III standing to pursue this action in federal court.

## 19   **II. LEGAL STANDARD**

20           Federal courts are courts of limited jurisdiction. Article III of the Constitution “confines  
21 the federal judicial power to the resolution of ‘Cases’ and ‘Controversies.’” *TransUnion LLC v.*  
22 *Ramirez*, 141 S. Ct. 2190, 2203 (2021). “For there to be a case or controversy under Article III,  
23 the plaintiff must have a ‘personal stake’ in the case – in order words, standing.” *Id.* (citation and  
24 quotation marks omitted). To establish standing, a “[p]laintiff must have (1) suffered an injury in  
25 fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to  
26 be redressed by a favorable judicial decision.” *Spokeo v. Robins*, 578 U.S. 330, 338 (2016). Here,  
27 traceability and redressability are not at issue.

28           “To establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a

1 legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not  
2 conjectural or hypothetical.’” *Id.* at 339 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560  
3 (1992)). The critical inquiry raised by Zynga is whether the injuries alleged are concrete. A  
4 “concrete” injury may include tangible or intangible harms, so long as they “actually exist” and  
5 are “‘real,’ and not ‘abstract.’” *TransUnion*, 141 S. Ct. at 2204 (quoting *Spokeo*, 578 U.S. at 340).  
6 A real, existing injury is a prerequisite to federal jurisdiction because “federal courts do not  
7 adjudicate hypothetical or abstract disputes,” nor do they “exercise general legal oversight . . . of  
8 private entities.” *Id.* at 2190.

9       The Court evaluates challenges to Article III standing under Rule 12(b)(1), which governs  
10 motions to dismiss for lack of subject matter jurisdiction. *See Maya v. Centex Corp.*, 658 F.3d  
11 1060, 1067 (9th Cir. 2011) (motion to dismiss for lack of standing governed by Rule 12(b)(1)).  
12 Rule 12(b)(1) motions may be either facial, where the inquiry is confined to the allegations in the  
13 complaint, or factual, where the court is permitted to look beyond the complaint to extrinsic  
14 evidence. *See Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014); *Safe Air For Everyone v.*  
15 *Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). When a defendant challenges jurisdiction “facially,”  
16 all material allegations in the complaint are assumed true, and the court determines whether  
17 the factual allegations are sufficient to invoke the court’s subject matter jurisdiction. *See Leite*,  
18 749 F.3d at 1121; *Meyer*, 373 F.3d at 1039. When a defendant makes a factual challenge “by  
19 presenting affidavits or other evidence properly brought before the court, the party opposing the  
20 motion must furnish affidavits or other evidence necessary to satisfy its burden of establishing  
21 subject matter jurisdiction.” *Meyer*, 373 F.3d at 1039; *see also Leite*, 749 F.3d at 1121. The court  
22 need not presume the truthfulness of the plaintiff’s allegations under a factual attack. *Wood v. City*  
23 *of San Diego*, 678 F.3d 1075, 1083 n.2 (9th Cir. 2011). The plaintiff must show by a  
24 preponderance of the evidence each requirement for subject-matter jurisdiction, and as long as  
25 the dispute is not intertwined an element of the plaintiff’s cause of action, the court may resolve  
26 any factual disputes itself. *Leite*, 749 F.3d at 1121.

27       Zynga purports to mount a factual attack by relying on the declaration of Zynga’s technical  
28 director filed in support of its first motion to dismiss. (Motion to Dismiss the SAC (“Mtn.”), Dkt.

1 No. 96, at 1 (citing Declaration of Jessup Ferris in Support of Motion to Dismiss, Dkt. No. 72-  
2 12.).) Although the instant motion cites to the Ferris declaration, the jurisdictional inquiry below  
3 does not turn on any factual dispute. Accordingly, the Court construes the 12(b)(1) motion as a  
4 facial attack.

5 In a class action, at least one named plaintiff must have standing. *See Frank v. Gaos*, 139  
6 S. Ct. 1041, 1046 (2019); *Ollier v. Sweetwater Union High Dist.*, 768 F.3d 843, 865 (9th Cir.  
7 2014). Thus, “if none of the named plaintiffs purporting to represent a class establishes the  
8 requisite of a case or controversy with the defendant[ ], none may seek relief on behalf of himself  
9 or any other member of the class.” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974). Moreover,  
10 standing must be established “for each claim that they press and for each form of relief that they  
11 seek (for example, injunctive relief and damages).” *TransUnion*, 141 S. Ct. at 2208. Because  
12 plaintiffs are the parties invoking federal jurisdiction, they “bear[ ] the burden of establishing these  
13 elements.” *Spokeo*, 578 U.S. at 338 (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)). In  
14 the absence of standing, there is no subject matter jurisdiction. *See Bender v. Williamsport Area*  
15 *Sch. Dist.*, 475 U.S. 534, 546–47 (1986) (citing *Mansfield C. & L.M.R. Co. v. Swan*, 111 U.S. 379,  
16 382 (1884)).

### 17 III. ANALYSIS

18 As noted above, plaintiffs seek both damages and injunctive relief for 29 causes of action  
19 under state statutory and common law. According to plaintiffs, they allege the following forms of  
20 harm: (i) a “present, increased risk” of identity theft; (ii) time spent mitigating said risk; (iii)  
21 emotional distress; (iv) diminution in value of their PII; and (v) loss of privacy. (Opposition to  
22 Motion to Dismiss (“Opp.”), Dkt. No. 98, at 9–24.)<sup>3</sup> Plaintiffs argue that each of these alleged  
23 injuries confers Article III standing.

24 Zynga contends that because plaintiffs have not demonstrated that the alleged harms are

---

26 <sup>3</sup> The harms described in plaintiffs’ opposition brief do not track the laundry list of  
27 injuries alleged in the SAC; nor do plaintiffs associate each of the alleged injuries with each of the  
28 claims. (*See Compl.* ¶¶ 139, 141–42, 183.) The Court declines to scour the 101-page pleading to  
do the same. Instead, the Court considers the alleged harms as described in plaintiffs’ opposition  
brief and assumes, for plaintiffs’ benefit, that all of the counts are premised on each of the alleged  
injuries.

1 concrete, they fail to establish an injury in fact and therefore lack Article III standing.  
2 Specifically, Zynga argues that plaintiffs cannot demonstrate standing: (1) based on the alleged  
3 risk of identity theft; (2) based on the alleged loss of privacy; and (3) for injunctive relief. As  
4 explained below, the other injuries alleged (mitigation costs, emotional distress, and diminution in  
5 value) rise and fall with the alleged risk of identity theft. Before evaluating these alleged injuries,  
6 the Court begins its analysis by observing recent guidance from the Supreme Court about whether  
7 an alleged harm is adequately concrete so as to confer Article III standing.

8 **A. *TRANSUNION LLC v. RAMIREZ***

9 In *TransUnion LLC v. Ramirez*, a class of plaintiffs sued the credit reporting company  
10 under the Fair Credit Reporting Act because their credit reports misleadingly labeled them as  
11 potential terrorists. *TransUnion*, 141 S. Ct. at 2200–02. TransUnion, however, provided the  
12 inaccurate reports to third parties for only a subset of plaintiffs. *Id.* The Supreme Court held that  
13 these plaintiffs suffered harm akin to defamation, enabling them to maintain their claims. *Id.* at  
14 2209; *see id.* at 2204 (“courts should assess whether the alleged injury to the plaintiff has a ‘close  
15 relationship’ to a harm ‘traditionally’ recognized as providing a basis for a lawsuit in American  
16 courts”) (quoting *Spokeo*, 578 U.S. at 341).

17 However, the same could not be said about the remaining plaintiffs whose credit reports  
18 TransUnion had never published to others. According to the Court, because defamation requires  
19 evidence of publication, which is traditionally “presumed to cause a harm, albeit not a readily  
20 quantifiable harm,” those plaintiffs’ failure to allege dissemination was fatal to their traditional-  
21 harm theory. *Id.* at 2211. In other words, “the mere presence of an inaccuracy in an internal credit  
22 file, if it is not disclosed to a third party,” does not closely resemble the harm associated with  
23 common law defamation and therefore “causes no concrete harm.” *Id.* at 2210.

24 Nor could that group of plaintiffs suffer a concrete injury based on the risk of harm where  
25 such risk of harm did not materialize (that is, dissemination of the inaccurate credit reports to third  
26 parties) or cause some other injury. *Id.* at 2211. The Supreme Court explained that “a person  
27 exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm  
28 from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.” *Id.* at

1 2210 at (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5). However, where a plaintiff  
 2 brings “a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a  
 3 concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate*  
 4 concrete harm.” *Id.* at 2210–11.

## 5 **B. ALLEGED INJURIES IN FACT**

6 Plaintiffs assert both theories of injury-in-fact discussed in *TransUnion*: a harm  
 7 traditionally recognized at common law as well as a risk of harm (or in plaintiffs’ words, a  
 8 “present, increased risk of harm”). The Court considers each in turn, beginning with the former.

### 9 **1. TRADITIONAL HARM: INVASION OF PRIVACY**

10 In *TransUnion*, the Supreme Court instructed that “courts should assess whether the  
 11 alleged injury to the plaintiff has a ‘close relationship’ to a harm ‘traditionally’ recognized as  
 12 providing a basis for a lawsuit in American courts,” such as physical harm, monetary harm, or  
 13 various intangible harms. *Id.* at 2204. Concrete intangible harms “include, for example,  
 14 reputation harms, disclosure of private information, and intrusion upon seclusion.” *Id.* (citations  
 15 omitted). This inquiry focuses on “whether plaintiffs have identified a close historical or  
 16 common-law analogue for their asserted injury . . . but does not require an exact duplicate in  
 17 American history or tradition.” *Id.* In addition to history, “Congress’s views may be  
 18 ‘instructive.’” *Id.* (quoting *Spokeo*, 578 U.S. at 341).

19 Plaintiffs submit that they allege invasions of privacy bearing a close relationship to harms  
 20 caused by the common law private torts of disclosure of private facts and intrusion upon seclusion.  
 21 As to the public disclosure of private facts, “[o]ne who gives publicity to a matter concerning the  
 22 private life of another is subject to liability to the other for invasion of his privacy, if the matter  
 23 publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not a  
 24 legitimate concern to the public.” Restatement (Second) of Torts § 652D. A plaintiff whose  
 25 private life is given publicity “may recover for the harm resulting to his reputation from the  
 26 publicity.” *Id.* § 652H. As to intrusion upon seclusion, “[o]ne who intentionally intrudes,  
 27 physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns,  
 28 is subject to liability to the other for invasion of his privacy, if the intrusion would be highly

1 offensive to a reasonable person.” *Id.* § 652B. A plaintiff who suffers an intrusion upon seclusion  
2 “may recover damages for the deprivation of his seclusion.” *Id.* § 652H.

3 Zynga challenges plaintiffs’ reliance on these traditional harms, arguing that plaintiffs fail  
4 to adequately allege (1) the disclosure of private facts and (2) publicity. The Court notes that for  
5 both torts, the harm is caused by the disclosure of or intrusion upon matters of a kind that would  
6 be “highly offensive to a reasonable person.” Even viewing the allegations in the light most  
7 favorable to plaintiffs, the Court finds that the type of harm they suffered as a result of the data  
8 breach is not analogous to the type of harm suffered as a result of private information. Plaintiffs  
9 have not demonstrated that the information stolen was of a nature that disclosure or intrusion  
10 thereupon would be highly offensive to the reasonable person. *Cf. TransUnion*, 141 S. Ct. at 2209  
11 (“The harm from being labeled a ‘potential terrorist’ bears a close relationship to the harm from  
12 being labeled a ‘terrorist.’”). The Court reasons:

13 First, the Court is hard pressed to conclude that basic contact information, including one’s  
14 email address, phone number, or Facebook or Zynga username, is private information. All of this  
15 information is designed to be exchanged to facilitate communication and is thus available through  
16 ordinary inquiry and observation. Next, “there is no liability for giving publicity to facts about the  
17 plaintiff’s life that are matters of public record, such as the date of his birth[.]” Restatement  
18 (Second) of Torts § 652D, Comment b. Finally, assuming it is not encrypted, the Zynga password  
19 presents a closer question as passwords generally are confidential. However, under the  
20 circumstances of this case, it is not clear to the Court, nor do plaintiffs explain, how the discovery  
21 of a password to a gaming account would be “highly offensive to a reasonable person,”<sup>4</sup>  
22 particularly where there is no allegation that the gaming accounts for which plain text passwords  
23 were taken contain confidential information.<sup>5</sup> It is also worth noting that plaintiffs do not allege  
24 that any of their actual first or last names were exposed in the data breach, suggesting that their

---

25  
26 <sup>4</sup> For example, will a player be offended if others learned their *Words With Friends*  
statistics?

27 <sup>5</sup> Whether the password can be used to commit identity theft is a different matter  
28 discussed in the next section.

1 anonymity is preserved.<sup>6</sup> Moreover, with the exception of a date of birth, which is immutable, all  
 2 of this information can be changed. Even when these pieces of information are considered  
 3 holistically, the Court does not view the collection of email addresses, phone numbers, Zynga  
 4 usernames, Zynga passwords, and Facebook usernames so private that their revelation would be  
 5 highly offensive to a reasonable person.<sup>7</sup>

6 In sum, while plaintiffs are not required to prove the elements for a common-law analogue  
 7 in order to secure standing,<sup>8</sup> they must demonstrate that the harm posed by the theft of their  
 8 information bears a “close relationship” to these traditionally recognized harms. *Cf TransUnion*,  
 9 141 S. Ct. at 2209 (“[T]he harm from a misleading statement of this kind bears a sufficiently close  
 10 relationship to the harm from a false and defamatory statement.”). Here, plaintiffs broadly assert  
 11 that “a combination of multiple categories information can convey a wealth of information and  
 12 seriously implicate privacy rights.” (Opp. at 22.)<sup>9</sup> However, in data breach cases, courts must  
 13 examine the nature of the specific information at issue to determine whether privacy interests were  
 14 implicated at all. Otherwise, every data breach (or any situation in which one loses control of  
 15 information) would confer standing, regardless of whether private information is exposed.

16 For the reasons stated above, the Court finds an insufficient fit between the loss of  
 17 information alleged here and the common law privacy torts of private disclosure of private facts

---

19 <sup>6</sup> Rosiak’s Facebook name was also allegedly taken, but he even concedes that he used a  
 20 fake first name on his Facebook profile. (SAC ¶ 121.)

21 <sup>7</sup> In their brief, plaintiffs make no mention of any privacy interests in the password reset  
 22 tokens, dates and times when the account was created and last accessed, or the IP address of the  
 last login. The Court will not address an issue not briefed by the parties.

23 <sup>8</sup> Nor are they required to demonstrate additional consequences from the invasion of  
 privacy, once shown, because the invasion itself constitutes the alleged injury in fact.

24 <sup>9</sup> The Court is not persuaded by plaintiffs’ reliance on cases involving the disclosure of a  
 25 plaintiff’s name and alleged debt to a third party. (Opp. at 20 (citing *Hunstein v. Preferred*  
 26 *Collection & Mgmt. Servs.*, 994 F.3d 1341, 1347 (11th Cir. 2021), *Thomas v. Unifin, Inc.*, No. 21-  
 27 *cv-3037* (SJC), 2021 WL 3709184 (N.D. Ill. Aug. 20, 2021), and *Keller v. Northstar Location*  
 28 *Servs.*, No. 21-cv-3389 (SJC), 2021 WL 3709183 (N.D. Ill. August 20, 2021).) All are factually  
 distinguishable. Plaintiffs’ names were not alleged to be stolen, and their contact information, date  
 of birth, and password for a gaming account are distinguishable from the fact and amount of one’s  
 debt.

1 and intrusion upon seclusion. Therefore, the Court agrees with Zynga that the privacy injuries  
2 alleged here are not sufficiently concrete to provide the basis for Article III standing.<sup>10</sup>

## 3 2. RISK OF HARM

### 4 a. STANDING TO SUE FOR DAMAGES

5 Zynga also argues that, in light of *TransUnion*, plaintiffs cannot rely on a “mere risk of  
6 future harm” as a basis for standing. Plaintiffs contend that they allege more than a mere risk of  
7 future harm but rather they allege a “present, increased risk” of harm. In the Court’s view,  
8 plaintiffs are drawing a distinction without a difference. Nowhere in *TransUnion* does the  
9 Supreme Court use this language or otherwise distinguish between a present risk of harm and a  
10 future risk of harm.<sup>11</sup> The point made by the Supreme Court is that a “pre-existing” risk of harm  
11 cannot confer Article III standing in a suit for damages. *See TransUnion*, 141 S. Ct. at 2211 (risk  
12 of harm, by itself, is not a sufficiently concrete injury). Thus, to the extent that plaintiffs base  
13 standing on a (present) risk of identity theft, they cannot pursue their claims for damages.

14 The Supreme Court explained that a risk of harm must either *materialize* or *cause some*  
15 *other injury* in order to confer standing in a suit for damages. *See id.* The Court therefore  
16 considers whether plaintiffs do, in fact, “allege more than” a risk of harm. Specifically, the Court  
17 evaluates whether the asserted risk of harm, here, identity theft, materialized or caused some other  
18 injury.

### 19 i. MATERIALIZATION OF RISK: ACTUAL IDENTITY THEFT

20 Plaintiffs argue that “the alleged risk of harm has actually materialized for” them. (Opp. at  
21

---

22 <sup>10</sup> Because the Court concludes that the disclosure and intrusion here are not highly  
23 offensive to a reasonable person, it necessarily finds that private facts are not at issue and therefore  
24 need not address Zynga’s challenge regarding plaintiffs’ purported failure to allege publicity.  
25 Nevertheless, even if the highly-offensive component were not met, the Court questions whether  
26 plaintiffs could establish that their alleged harm bears a “close relationship” with the harm  
27 resulting from a public disclosure of private facts without any showing of “harm to their reputation  
28 from the publicity,” assuming publicity occurred here. Moreover, plaintiffs allege that a third-  
party hacker, not Zynga, stole their information and therefore it is doubtful whether they can show  
that Zynga (whom plaintiffs sue for negligence) directly harmed them in a way that is analogous to  
the harm from *intentional* intrusion upon seclusion.

<sup>11</sup> If there is a risk of some event, then there is a currently existing possibility that that  
event will occur in the future.



1 6.) The Court disagrees. The harm to which plaintiffs refer is identity theft (or fraud). Thus, the  
2 materialization of the risk of identity theft is *actual* identity theft, not *attempted* identity theft. *See*  
3 *id.* (“[T]he 6,332 plaintiffs did not demonstrate that the risk of future harm materialized—that is,  
4 that the inaccurate OFAC alerts in their internal TransUnion credit files were ever provided to  
5 third parties or caused a denial of credit.”).<sup>12</sup>

6 Here, the SAC does not allege that any of the plaintiffs actually experienced any type of  
7 fraud or identity theft as a result of the data breach, such as the unauthorized access of an account  
8 or the unauthorized transaction made in their name. Notwithstanding, plaintiffs argue that their  
9 information “has been used to compromise their other accounts with credential stuffing, to  
10 establish new accounts in their names, to entice them with phishing emails from purported banks  
11 and brokerage companies, to lure them with personal emails meant to look like a personal  
12 conversation, and to bombard them with spam calls and texts.” (Opp. at 1.) As an initial matter,  
13 in light of *TransUnion*, the Court concludes that mere compromise of personal information,  
14 without more, fails to satisfy the injury-in-fact element in the absence of an identity theft.  
15 Moreover, the Court finds that being “entice[d]” or “lure[d]” into giving information that can be  
16 used to commit fraud is not the same thing as actually being defrauded. Further, the Court agrees  
17 with other courts that “receiving spam or mass mail does not constitute an injury in fact.” *See, e.g.*  
18 *Jackson v. Loews Hotels, Inc.*, No. 18-cv-827 (DMG), 2019 WL 6721637, at \*4 (C.D. Cal. July  
19 24, 2019) (citing cases including *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y.  
20 2009) (“The receipt of spam by itself . . . does not constitute a sufficient injury entitling [the  
21 plaintiff] to compensable relief.”)).

22 Finally, the SAC does not plausibly allege that unauthorized accounts were established in  
23 any of the plaintiffs’ names. Plaintiffs argue that “I.C.’s identity has already been stolen to set up  
24 fraudulent accounts with financial information.” (Opp. at 12 (citing SAC ¶ 11 and related  
25

---

26 <sup>12</sup> The Court is not persuaded by plaintiffs’ characterization of attempted identity theft as  
27 actual misuse of their stolen information. (Opp. at 8 (“Plaintiffs assert damages based on *actual*  
28 *misuse* of their PII by cybercriminals attempting to commit identity theft and fraud—a *present*  
risk of harm.”), 12 (“Plaintiffs’ PII *has already been misused*—specifically, to target Plaintiffs in  
an attempt to commit identity theft and fraud.”).)

1 screenshot.) Putting aside the fact that the SAC does not plausibly allege that any of I.C.’s  
 2 information stolen in the data breach could be used to set up an account with a financial  
 3 institution, such as a social security number, nothing in the non-personalized message, reproduced  
 4 above, plausibly suggests that I.C.’s identity was actually stolen to create a fraudulent account.  
 5 The Court also notes that the SAC contains vague allegations regarding “unauthorized access to  
 6 and misuse of their accounts, “lowered credit scores resulting from credit inquiries and caused by  
 7 fraudulent activities,” and “unauthorized charges and loss of use of and access to their financial  
 8 account funds and costs associated with inability to obtain money from their accounts or being  
 9 limited in the amount of money they were permitted to obtain from their accounts, including  
 10 missed payments on bills and loans, late charges and fees, and adverse effects on their credit.”  
 11 (SAC ¶¶ 142 (d), (e), 183(d).) However, the SAC does not allege that any of the plaintiffs actually  
 12 experienced any of these adverse consequences, information that they would presumably know  
 13 especially given that the breach occurred at the end of 2019 and the most recent version of the  
 14 complaint was filed at the end of August 2021.

15 Therefore, because plaintiffs do not allege any actual identity theft or fraud, they cannot  
 16 claim an injury in fact based on a materialization of the risk of harm. *See TransUnion*, 141 S. Ct.  
 17 at 2211.

#### 18 **ii. OTHER INDEPENDENT INJURIES CAUSED BY RISK OF HARM**

19 Plaintiffs also do not plausibly allege other independent injuries caused by the risk of  
 20 identity theft. Plaintiffs cite the following as other injuries: credential stuffing; phishing attacks;  
 21 unsolicited emails, text messages, robocalls and other spam; mitigation costs; emotional distress;  
 22 and diminution in value of the information taken.<sup>13</sup>

---

23  
 24 <sup>13</sup> Plaintiffs also allege “theft of their PII” and benefit of the bargain losses (SAC ¶¶  
 25 142(a), 258) but do not address these alleged harms in their briefing. The Court declines to rule  
 26 on issues not briefed by the parties. In any event, the Court is doubtful that either of these alleged  
 27 injuries to be sufficiently concrete, as the SAC lacks any allegation that the information stolen was  
 28 of any economic value *to plaintiffs*. Thus, it is unclear how plaintiffs suffered from “theft of their  
 PII” apart from the other injuries discussed above, and without an exchange of value for the  
 allegedly bargained-for data security, there can be no injury in fact based on a benefit of the  
 bargain loss.

1 First, with respect to credential stuffing, phishing attacks, and the various forms of spam,  
2 the Court views these tactics as targeted *attempts* to commit identity theft. As stated above, the  
3 Court finds these attempts fall short of actual identity theft. Further, the source of these  
4 unsolicited contacts is hard to track. Even assuming that these acts are fairly traceable to the  
5 Zynga data breach, plaintiffs do not allege that any of these attempts succeeded, again something  
6 they would presumably know. Because these alleged harms merely present a risk of identity theft,  
7 they cannot plausibly be considered independent injuries.

8 Second, with respect to mitigation costs and emotional distress, Zynga argues that the risk  
9 of harm giving rise to these alleged injuries is “speculative,” whereas plaintiffs contend that such  
10 risk is “substantial.” (Mtn. at 10; Opp. at 12.) These injuries can only qualify as concrete injuries  
11 in fact when they are based on a risk of harm that is either “certainly impending” or “substantial.”  
12 *See Clapper*, 568 U.S. at 422 (plaintiffs “cannot manufacture standing by incurring costs in  
13 anticipation of non-imminent harm”); *Payne v. Off. of the Cmm’r of Baseball*, 705 F. App’x 654,  
14 655 (9th Cir. 2017) (rejecting argument that plaintiffs’ “general anxiety about being injured by  
15 foul balls constitutes an injury-in-fact, because it is based on ‘fears of hypothetical future harm  
16 that is not certainly impending’”) (quoting *Clapper*, 568 U.S. at 416). Thus, no Article III  
17 standing exists if a plaintiff’s theory of injury rests on an “attenuated chain of inferences necessary  
18 to find harm.” *Clapper*, 568 U.S. at 414 n.5.

19 Given the nature of the information at issue, the Court agrees with Zynga and finds that the  
20 risk of harm which caused the asserted costs and stress is too conjectural such that they cannot  
21 qualify as concrete injuries of fact. For one thing, the Court questions whether criminals would be  
22 able to use e-mail addresses, Zynga usernames and Zynga passwords, Facebook username, phone  
23 numbers, and dates of birth, even collectively, to commit identity theft. The SAC does not allege  
24 that Zynga collected, or that plaintiffs stored in their accounts, their payment or other financial  
25 information. It is unclear how a third party could make a credit inquiry, set up a new bank account  
26 or access an existing one, apply for a loan, or commit some other fraud without more information,  
27 such as first and last names or social security number.

28 While the SAC alleges this information is susceptible to fraudulent use by way of phishing

1 attacks and credential stuffing, the Court finds this notion implausible. According to the SAC, the  
 2 information stolen “includes enough information to potentially create targeted phishing attacks  
 3 made up to look as they are an official communication from Zynga,” (SAC ¶ 101) (internal  
 4 quotation marks and citation omitted), but phishing, by its nature, demonstrates that the limited  
 5 information disclosed is not enough. The Court would therefore still need to speculate that  
 6 plaintiffs will be successfully duped by a phishing attack and that the additional information  
 7 turned over as a result can be used to commit identity theft, which the SAC does not allege.

8           Credential stuffing also requires a series of assumptions to conclude that identity theft is  
 9 substantially likely in this case. Johnson is the only named plaintiff whose plain text Zynga  
 10 password was allegedly stolen and who used that same password “for many other online accounts,  
 11 including her email account which she uses to send confidential information such as financial  
 12 information and communications with her doctor’s office.” (SAC ¶ 20.) The SAC alleges that she  
 13 and her sister “went through every online account she could think of that had the same password  
 14 as her Zynga account.” (*Id.*) I.C. also allegedly used his Zynga password “for approximately 90%  
 15 of his online accounts, including email, entertainment, gaming, social media popular with youth,  
 16 and others.” (*Id.* ¶ 105.) Though the SAC does not allege that I.C.’s password was taken in plain  
 17 text form, it does allege that online websites “explain[ed] how to crack the Zynga hashed  
 18 passwords” (*id.* ¶ 72 (citations omitted)), which were already encrypted with an “outdated and  
 19 insecure” encryption method. (*Id.* ¶ 71 (internal quotation marks and citation omitted).) I.C. also  
 20 changed his account passwords and installed two-factor authenticational application for his accounts  
 21 but “cannot be certain” that he did this for all of his accounts. (*Id.* ¶ 118.)<sup>14</sup> The Court would  
 22 therefore need to assume, at minimum, that (1) Johnson or I.C. have forgotten some account; (2) a  
 23 third party could successfully access that account, for example, because plaintiffs paired the  
 24 forgotten account’s password with one of the other pieces of information taken in the breach; and  
 25 (3) that other account could be used to consummate an unauthorized transaction. *See, e.g., B.J.F.*

26  
 27 \_\_\_\_\_  
 28 <sup>14</sup> Although Rosiak’s Zynga hashed password was also allegedly taken, there is no  
 allegation that he used the same password for his other accounts.

1 v. *PNI Digital Media*, No. 15-cv-1643 (MJP), 2016 WL 4014113, at \*2 (W.D. Wash. July 27,  
2 2016) (finding no standing even where the plaintiff alleged that she had used the same password  
3 because she did not “describe the nature of the accounts that she used the same password for” or  
4 “explain how she would be harmed if those other accounts were accessed by hackers”). The Court  
5 declines to find a “certainly impending” risk of harm based on a chain of unsupported inferences.  
6 Because plaintiffs do not show a substantial or imminent risk of identity theft, they cannot rely on  
7 the resulting mitigation expenses or emotional distress to secure standing.<sup>15</sup>

8 Third, with respect to the devaluation of the information stolen, the Court finds that  
9 plaintiffs do not adequately allege such an injury. “The Ninth Circuit has recognized diminution  
10 in value of personal theory as a viable theory of damages under state contract law.” *Svenson v.*  
11 *Google Inc.*, No. 13-cv-4080 (BLF), 2016 WL 8943301, at \*9 (N.D. Cal. Dec. 21, 2016) (citing  
12 *Facebook Privacy Litig.*, 572 F. App’x 494, 494 (9th Cir. 2014). “In order to show injury in fact  
13 under this theory, [plaintiffs] must establish both the existence of a market for [their] personal  
14 information and an impairment of [their] ability to participate in that market.” *Id.* (citing *In re*  
15 *Google, Inc. Privacy Policy Litig.*, No. 12-cv-1382 (PSG), 2015 WL 4317479, at \*4 (N.D. Cal.

16  
17 <sup>15</sup> Plaintiffs point to previous Ninth Circuit cases where the threat of identity theft  
18 constituted an injury in fact and argues that the Court should similarly find an injury in fact in this  
19 case. See *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023 (9th Cir. 2018) (hackers’ theft of “the  
20 names, account numbers, passwords, email addresses, billing and shipping addresses, telephone  
21 numbers, and credit-card and debit-card information of more than 2 million Zappos customers”  
22 constituted a substantial risk of future harm); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140,  
23 1143 (9th Cir. 2010) (plaintiffs had alleged “a credible threat of harm” stemming from the theft of  
24 a laptop containing “the unencrypted names, addresses, and social security numbers of  
25 approximately 97,000 Starbucks employees”). Indeed, this Court is aware that the Ninth Circuit in  
26 *Zappos* credited the plaintiffs’ allegations that they were at a higher risk of “phishing” and  
27 “pharming” as a result of the data breach. *Zappos*, 888 F.3d at 1027. However, the information  
28 exposed in those cases provided the third parties with a clear ability to commit fraud or identity  
theft and therefore is distinguishable from the stolen information in the instant case, which, for the  
reasons stated above, the Court finds cannot, without more, plausibly be used to commit fraud.

More fundamentally, 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*’s holdings  
finding standing on this very basis.

Finally, the Court is mindful of the procedural posture of *TransUnion*, as pointed out by  
plaintiffs, but does not consider the fact that *TransUnion* had proceeded to a jury verdict dictates a  
different result in this case. Indeed, at this stage, the Court accepts all the allegations as true and  
views them in the light most favorable to plaintiffs.

1 July 15, 2015)). Even assuming the existence of a market for the information taken in this case,<sup>16</sup>  
 2 the SAC is devoid of any allegations describing how the breach devalued plaintiffs’ specific  
 3 information, that is, email addresses, Zynga usernames and passwords, phone numbers, dates of  
 4 birth, or Facebook username, such that they are prevented from deriving economic benefit from  
 5 this information in the future. *See, e.g., In re Facebook, Inc. Consumer Privacy User Profile*  
 6 *Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) (plaintiffs failed to “plausibly allege that  
 7 someone else would have bought [their non-disclosed personal information] as a stand-alone  
 8 product”). “[P]laintiffs’ economic-loss theory is therefore purely hypothetical and does not give  
 9 rise to standing.” *Id.* (citing cases).

10 In sum, plaintiffs have not alleged that they were victims of actual identity theft, nor have  
 11 they pled any other injuries caused by the risk of identity theft that are sufficiently concrete.  
 12 Accordingly, under *TransUnion*, plaintiffs fail to allege standing to sue for damages and therefore  
 13 all such claims are **DISMISSED**.

#### 14 b. STANDING TO SUE FOR INJUNCTIVE RELIEF

15 The Court also must consider whether plaintiffs have standing to request injunctive relief.  
 16 As stated above, a “person exposed to a risk of future harm may pursue forward-looking,  
 17 injunctive relief to prevent harm from occurring, at least so long as the risk of harm is sufficiently  
 18 imminent and substantial.” *TransUnion*, 141 S. Ct. at 2210 (citing *Clapper*, 568 U.S. at 414 n.5);  
 19 *see also Bates v. United Parcel Service, Inc.*, 511 F.3d 974, 985 (standing inquiry for injunctive  
 20 relief requires plaintiffs to “demonstrate that [they have] suffered or [are] threatened with a  
 21 ‘concrete and particularized’ legal harm, coupled with a ‘sufficient likelihood that [they] will  
 22 again be wronged in a similar way.’”) (quoting *Lujan*, 504 U.S. at 560, and *City of Los Angeles*,  
 23 461 U.S. 95, 111 (1983)). Zynga argues that plaintiffs “cannot show any imminent risk of future

---

24  
 25 <sup>16</sup> Plaintiffs’ counsel offers a declaration attesting to both the underground and legitimate  
 26 “marketplaces through users can monetize their personal information.” (Declaration of Mark  
 27 Clifford in Support of Opposition to Motion to Dismiss, Dkt. No. 98-1, ¶ 22.) The declaration  
 28 attaches an expert report filed in another case which “highlight[s] the various means by which the  
 value of compromised PII may be calculated and how consumers themselves can realize this  
 value” and notes that “[t]he types of PII described in [the] report are some of the same types of PII  
 compromised in the Zynga data breach.” (*Id.* ¶¶ 23–27.) None of these averments, however, are  
 included in the SAC, nor do they address plaintiffs’ specific information.

1 harm from *this* data breach.” (Mot. at 19.) For the reasons stated in Section III.B.2.a.ii, the Court  
2 agrees. Because the risk of harm here is not sufficiently imminent or substantial to confer  
3 standing, not even for a claim seeking purely injunctive relief, the Court **DISMISSES** all such  
4 claims.<sup>17</sup>

#### 5 **IV. CONCLUSION**

6 In short, plaintiffs fail to allege a concrete injury in fact and therefore lack constitutional  
7 standing to pursue their claims in federal court. The Court does not take lightly the serious harm  
8 suffered when one’s identity is stolen, especially that of a minor, and does not suggest that a  
9 plaintiff must always wait until this happens before seeking relief in federal court following a data  
10 breach. However, not every data breach creates a concrete injury, particularly where, as here, the  
11 information allegedly stolen has not be shown to be either so private that a reasonable person  
12 would be offended if exposed or so sensitive that it could be enough to commit identity theft.

13 Plaintiffs have already amended their pleadings after Zynga’s prior motion to dismiss, and  
14 they fail to show how amendment could demonstrate a cognizable injury suffice to support Article  
15 III standing. Because Article III standing is an essential ingredient for subject matter jurisdiction  
16 in federal court, the motion to dismiss for lack of subject matter jurisdiction is **GRANTED**, and the  
17 case is **DISMISSED WITH PREJUDICE**.<sup>18</sup>

18 This Order terminates Docket Number 96 and closes the case.

19 **IT IS SO ORDERED.**

20 Dated: April 29, 2022

21   
22 YVONNE GONZALEZ ROGERS  
23 UNITED STATES DISTRICT COURT JUDGE

24 <sup>17</sup> Plaintiffs correctly point out that Zynga does not challenge their standing for  
25 declaratory relief. Notwithstanding, the Court has an independent obligation to confirm its subject  
26 matter jurisdiction. *See FW/PBS*, 493 U.S. at 231. For the same reason that plaintiffs lack  
27 standing to pursue injunctive relief, namely, failure to demonstrate that the asserted risk of harm is  
28 sufficiently imminent or substantial, the Court concludes that they also lack standing to pursue  
29 declaratory relief.

<sup>18</sup> In reaching its decision, the Court did not have to rely on any matters contained in  
Zynga’s request for judicial notice or plaintiffs’ administrative motion to file a surreply. (Dkt.  
Nos. 97, 103.) Accordingly, those requests are **DENIED AS MOOT**.