

**IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

JEONG-SU KIM, HUE-SOUNG JUN,)
and JONG MIN LEE on behalf of)
themselves and all others similarly)
situated,)

Plaintiff,)

v.)

McDONALD’S USA, LLC, a Delaware)
limited liability company, and)
McDONALD’S CORPORATION,)
a Delaware corporation,)

Defendants.)

Case No. 21-cv-05287

Judge John Robert Blakey

MEMORANDUM OPINION AND ORDER

In this putative class action, Plaintiffs Jeong-Su Kim, Hue-Soung Jun, and Jong Min Lee assert claims against Defendants McDonald’s USA, LLC and McDonald’s Corporation for violating the Illinois Consumer Fraud Act (“ICFA”), 815 ILCS 505/1 *et seq.*, the Illinois Deceptive Trade Practices Act (“IDTPA”), 815 ILCS 510/1 *et seq.*, and the Republic of Korea’s Personal Information Protection Act (“PIPA”), alleging that Defendants’ negligence and misrepresentation that Plaintiffs’ personal information would be encrypted led to the theft of Plaintiffs’ names, email addresses, and street addresses from a database maintained by Defendants. Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), McDonald’s now moves to dismiss [18] Plaintiffs’ three-count complaint [1] in its entirety for lack of

Article III standing and for failure to state a claim. For the reasons explained below, the Court grants Defendants' motion based upon a lack of Article III standing.

I. Factual Allegations

A. The McDelivery App

The Court takes the following facts from Plaintiffs' complaint, [1], and assumes them to be true for purposes of Defendants' motion to dismiss.

McDonald's USA, LLC is a wholly owned subsidiary of Defendant McDonald's Corporation, which is incorporated in Delaware and has its principal place of business in Illinois. [1] ¶¶ 17, 18. Plaintiffs Jeong-Su Kim, Hue-Soung Jun, and Jong Min Lee, all of whom are residents of the Republic of Korea, used their personal information to register for an account ("McDelivery") with Defendants that would allow them to place delivery orders through Defendants' mobile app and Defendants' website. *Id.* ¶¶ 14, 15, 16, 56.

To register for delivery orders on McDelivery, Plaintiffs were required to provide their addresses, email addresses, and cell phone numbers. *Id.* ¶ 57. As part of the registration process, Defendants required users to agree to Defendants' terms and conditions, including their privacy policies. *Id.* ¶¶ 58, 94. To cater to both Koreans and non-Koreans living in Korea, the registration process for McDelivery is available in both Korean and English. *Id.* ¶ 59. The Korean language version of the privacy policy notifies users that their personal information—names, phone numbers, passwords, and email and delivery addresses—would be encrypted and secured when it is transmitted to Defendants in Illinois as well as to Amazon Web Services. *Id.*

¶ 60. Additionally, the privacy policy represents to its users that their personal information would be destroyed after one year of non-use. *Id.* ¶¶ 77, 97.

B. The Data Breach

On April 15, 2021, unknown third-party hackers stole McDelivery users' delivery addresses, phone numbers, and email addresses. *Id.* ¶ 1. Defendants delayed nearly two months in notifying their customers of the data breach. *Id.* ¶ 74. On June 13, 2021, Defendants published a notice on their webpage stating that unauthorized individuals obtained a file containing the email addresses, phone numbers, and physical addresses of their McDelivery customers. [1] ¶ 27. In the notice, Defendants stated that they had inspected their vulnerable servers and implemented security measures after learning of the data breach but advised the public to be cautious of phishing attempts and email solicitations from entities impersonating Defendants. *Id.* The notice reminded the public that Defendants do not request credit card and other financial information through phone or email and informed the public of a website where customers could confirm whether the data breach had compromised their personal information. *Id.*

On June 19, 2021, Defendants distributed an email to individual customers affected by the data breach containing the same information in the public notice, as well as an apology for their delay in identifying and notifying the individual customers of the data breach. *Id.* ¶ 28. The customers affected by the McDelivery data breach included not just Korean citizens but also U.S. citizens and individuals

who were living in or visiting the Republic of Korea, the Republic of China, South Africa, and Russia. *Id.* ¶ 29.

Plaintiffs Kim, Jun, and Lee learned from media outlets that their personal information was stolen in the data breach. *Id.* ¶¶ 14, 15, 16. Plaintiff Kim experienced an exponential increase in the amount of unwanted spam emails after the data breach and contacted McDonald’s customer service. *Id.* ¶ 14. In response to Kim, McDonald’s stated that it had strengthened its security measures but was unable to confirm whether Kim’s personal information was encrypted or secured when it was transferred to McDonald’s servers. *Id.* ¶ 14, 61.

Plaintiff Jun has received frequent notifications of unauthorized attempts to login to his email account from Japan. *Id.* ¶ 15. Additionally, even though Jun’s McDelivery account should have been deleted after a year of non-use, McDonald’s informed him that “due to a serious internal error,” his personal information had in fact been leaked during the data breach. *Id.* ¶¶ 15, 98–99, 107–08, 132. As a result, Jun spent time filing a police report regarding the data breach and in dealing with the unauthorized login attempts into his email account. *Id.* ¶ 15.

On August 13, 2021, four months after the data breach, Plaintiff Lee received an email entitled “Your Smartphone,” which informed Lee that “a website with his account . . . was hacked” and, as a result, the sender of the email was able to access Lee’s password and “cloud storage.” [1] ¶ 50. The email also informed Lee that the author of the email obtained Lee’s “very personal and inappropriate” files and

threatened to release these files to Lee's friends and colleagues unless Lee clicked on a link in the email and wired \$1,700. [1] ¶¶ 51–54.

Plaintiffs allege that, due to Defendants' failure to adequately safeguard and protect the "file" containing Plaintiffs' personal information, cybercriminals accessed, obtained, and used their personal information without authorization and invaded Plaintiffs' privacy. *Id.* ¶ 36. Further, Plaintiffs contend that, as a direct and proximate cause of the data breach, hackers may use that information to conduct phishing schemes against Plaintiffs, which are prevalent in Korea where Plaintiffs reside. *Id.* ¶¶ 45, 49. As alleged in the complaint, "phishing" is the practice of sending emails or text messages, purportedly from reputable companies or individuals, to induce the recipients into revealing personal information such as passwords and credit card numbers. *Id.* ¶¶ 6 n.1, 46. Since the data breach, Defendants have not offered Plaintiffs any compensation or direct personal protection from the data breach (such as the means to prevent phishing scams and identity theft insurance). *Id.* ¶ 67.

On October 5, 2021, Plaintiffs filed suit in this Court asserting claims against Defendants for violations of Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/*et seq.*, Illinois' Uniform Deceptive Trade Practices Act, 815 ILCS 510/*et seq.*, and the Republic of Korea's Personal Information Privacy Act. [1] ¶¶ 91–101, 102–116, 117–137. Plaintiffs allege that, as a result Defendants' failure to safeguard their personal information, third parties accessed their personal information without consent and are able to use Plaintiffs' email addresses to register for website subscriptions exposing them to countless spam and other unwanted

emails. *Id.* ¶¶ 6, 79. In addition, Plaintiffs remain at risk of phishing scams because their phone numbers are tied to their names and addresses. *Id.* ¶ 7. As a result, Plaintiffs have lost time and incurred expenses and mental aggravation monitoring their email accounts for phishing scams, removing spam emails, removing accounts registered on unwanted and unfamiliar websites, and communicating with McDonald's regarding their personal information stolen in the data breach, all of which has caused Plaintiffs anxiety, emotional distress, and loss of privacy. *Id.* ¶¶ 1, 9, 36, 37, 66, 79, 100, 115. Plaintiffs, individually and on behalf of all individuals who registered for McDelivery while in Korea, seek equitable relief, damages, attorneys' fees, and costs. *Id.* ¶¶ 81, 101, 116, 137.

Defendants now move to dismiss Plaintiff's complaint in its entirety under Rule 12(b)(1), arguing that Plaintiffs failed to allege an injury-in-fact necessary for Article III standing. In the alternative, Defendants move to dismiss Plaintiffs' complaint under Rule 12(b)(6) for failure to state a claim. [19] at 6–7. The Court begins with Defendants' challenge to the Court's subject matter jurisdiction. *See McCready v. White*, 417 F.3d 700, 702 (7th Cir. 2005) (“Ensuring the existence of subject-matter jurisdiction is the court's first duty in every lawsuit.”).

II. Legal Standard

A motion to dismiss under Rule 12(b)(1) challenges the Court's subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). If, as here, a defendant challenges the facial sufficiency of a complaint's allegations regarding the Court's subject matter jurisdiction, the Court must accept as true all well-pled factual allegations and draw

all reasonable inferences in the plaintiff's favor. *Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443–44.

III. Analysis

Defendants argue that Plaintiffs fail to allege an injury-in-fact and thus lack standing. [19] at 5. The standing requirement is rooted in Article III of the U.S. Constitution, which limits the subject matter jurisdiction of federal courts to “Cases” and “Controversies.” U.S. Const. Art. III, § 2; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (“the core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III.”). To meet the “irreducible constitutional minimum of standing,” a plaintiff must show 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, 334 (2016) (citing *Lujan*, 504 U.S. at 560–61).

The burden of establishing standing rests with the party invoking federal jurisdiction and, at the pleading stage, that party must “clearly . . . allege facts demonstrating each element.” *Id.* at 338 (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)). In a class action, the named plaintiffs representing a class “must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent,” *Warth*, 422 U.S. at 502, and “if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the

defendants, none may seek relief on behalf of himself or any other member of the class,” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974).

Relevant here, an injury-in-fact is “an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560 (cleaned up). “Concrete” means an injury that is “real” and not abstract—the injury “must actually exist,” and an injury is “particularized” if it affects the plaintiff “in a personal and individualized.” *Spokeo, Inc.*, 578 U.S. at 339–40.

In response to Defendants’ challenge, Plaintiffs argue that they pled concrete and particularized injuries when they alleged that: (1) they face an increased risk of identity theft and phishing scams as a result of Defendants’ negligence; (2) they suffer from anxiety, emotional distress, loss of privacy, and continue to spend time and efforts monitoring, reporting, and removing unwanted phishing scam emails; (3) the disclosure of their personal information has resulted in a loss of privacy; and (4) Defendants unlawfully retained Plaintiff Jun’s personal information in violation of PIPA. [20] at 7. The Court addresses each argument in turn.

A. Risk of Future Harm

First, Plaintiffs argue that the theft of their email addresses, phone numbers, and delivery addresses places them at an increased risk of becoming the victims of phishing scams and identity theft in the future. [20] at 7.

In *Clapper v. Amnesty Int’l USA*, the Supreme Court held that the plaintiffs, who sued to enjoin a federal statute that would potentially subject them to surveillance by the federal government, did not have standing to enjoin the

enforcement of the statute. 568 U.S. 398, 407 (2013). The Court held that, to have Article III standing, the “threatened injury must be *certainly impending* to constitute injury in fact,” and the plaintiffs’ theory of future harm—their assumption that the government would surveil their communications—“relied on a highly attenuated chain of possibilities” and “speculation about the decisions of independent actors,” such as whether the government would choose to target the plaintiffs for surveillance in the first place and whether a Foreign Intelligence Surveillance Court would authorize the government’s request for such surveillance. 586 U.S. at 410, 414 (cleaned up).

Relying on *Clapper*, the Seventh Circuit addressed the injury-in-fact requirement in the data breach context in *Remijas v. Nieman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). In *Remijas*, a data breach led to the disclosure of 350,000 credit cards used by Plaintiffs at defendant’s department stores, with 9,200 of the 350,000 cards being used fraudulently. *Remijas*, 794 F.3d at 690. The plaintiffs sued, arguing that they had suffered an injury-in-fact because the data breach placed them at an increased risk of identity theft. *Id.* at 693. The Seventh Circuit held that, for purposes of Article III standing, the plaintiffs had plausibly alleged a concrete and particularized injury because the data breach had placed the plaintiffs at a “substantial risk” of identity theft and credit card fraud—the data breach had already resulted in the disclosure of sensitive credit card information and 9,200 of the disclosed credit cards had already experienced fraudulent charges—and because the

plaintiffs had mitigation expenses associated with the effects of the data breach. *Id.* at 693–94.

Shortly after *Remijas*, the Seventh Circuit again held that a substantial risk of identity theft and fraud in the data breach context remained sufficiently concrete to satisfy Article III standing. *See Lewert v. P. F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016). In *Lewert*, the court found that the plaintiffs had standing to sue because it was “plausible to infer a substantial risk of harm from the data breach” because the stolen credit card information placed the plaintiffs at risk for both fraudulent charges and identity theft, one of the named plaintiffs had already experienced fraudulent charges on his credit card, and the plaintiffs incurred mitigation expenses related to the aftermath of the data breach. *Id.* at 965, 66.

Just last year, however, the Supreme Court clarified, in *Transunion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), that the “certainly impending” risk of future harm applied only to claims seeking forward-looking injunctive relief and that the risk of future harm, standing alone, cannot constitute an injury-in-fact for Article III purposes in a lawsuit seeking damages. *See TransUnion*, 141 S. Ct. at 2210–10. *TransUnion* involved claims that defendants maintained inaccurate credit reports in violation of the Fair Credit and Reporting Act, some of which were disclosed to third parties and some of which were not. *Id.* at 2201. The Court held that plaintiffs whose credit reports were disclosed suffered an injury similar to the tort of defamation because the inaccurate credit reports indicated that these plaintiffs’ names potentially matched names on a government-maintained list of terrorists, drug

traffickers, and other serious criminals, which was sufficient to demonstrate a concrete injury for purposes of Article III. *Id.* at 2208. The plaintiffs whose reports were not disclosed, however, did not, even though they faced a risk of future disclosure. *Id.* at 2210. The Court held that the risk of future disclosure was too speculative to constitute a concrete injury-in-fact in a claim for damages; the Court held that the disclosure, not the risk of disclosure, constitutes the injury. *See id.* at 2210–11.

Following *TransUnion*, the Seventh Circuit has subsequently held that the threat of future harm alone cannot satisfy Article III standing, at least in a lawsuit for money damages. *See Ewing v. MED-1 Solutions, LLC*, 24 F.4th 1146, 1152 (7th Cir. 2022) (“*TransUnion* makes clear that a risk of future harm, without more, is insufficiently concrete to permit standing to sue for damages in federal court.”); *Pierre v. Midland Credit Mgmt, Inc.*, 29 F.4th 934, 938 (7th Cir. 2022) (“A plaintiff seeking money damages has standing to sue in federal court only for harms that have in fact materialized.”).

Here, none of the Plaintiffs have alleged that they, in fact, fell victim to a phishing scam or otherwise had their identities stolen. Plaintiff Lee alleges that he received a phishing email that threatened to release “very personal and inappropriate” files to his friends, [1] ¶¶ 50–54, but Lee does not allege that the sender of the email had, in fact, gained any access to his files, nor does he allege that he paid the sender of the phishing email any money or that any files were released. Indeed, Plaintiffs’ response brief concedes that Lee recognized the phishing email for

what it was—an attempt. *See* [20] at 8 n.2 (“Plaintiff Lee has had to spend time monitoring unwanted e-mails and even extortion *attempts*.”) (emphasis added)). Similarly, Plaintiff Jun alleges only that he received notifications that an individual in Japan had “*attempted*” to log in to his email, but he does not allege that any of the log in attempts succeeded. [1] ¶ 15. And Plaintiff Kim alleges only that he experienced an uptick in the number of unwanted spam emails after he was notified of the data breach. [1] ¶ 14.

With respect to potential future harms, Plaintiffs fail to plausibly allege that the harm they fear—identity theft and being victimized by a phishing scam—is impending. The type of data stolen in the data breach consisted of non-sensitive email addresses, phone numbers, and delivery addresses. [1] ¶ 27. Unlike the plaintiffs in *Remijas* and *Lewert*, which involved stolen credit card information that led to plaintiffs experiencing actual fraud, the harm Plaintiffs claim here remains too attenuated and speculative given the non-sensitive nature of the information stolen in the data breach. For instance, unless Plaintiffs used their cell phone numbers or street addresses as the passwords for their email or other accounts (which they do not allege), potential hackers would still need to resort to other methods to gain access to Plaintiffs’ accounts. The claimed future harm would require a “highly attenuated chain of possibilities” to materialize and finding such harm would “require guesswork as to how independent decisionmakers will exercise their judgment.” *Clapper*, 568 U.S. at 410, 413.

As for Plaintiffs’ fears of falling victim to phishing scams, only Plaintiff Lee alleges that he was the victim of a phishing attempt. [1] ¶¶ 50–55. Again, assuming that the email Lee received was “fairly traceable” to the data breach, this lone email is not sufficient to indicate that his fear of falling victim to a phishing scam is “certainly impending,” particularly where he does not allege that the sender of the email had actually gained access to his personal files. [1] ¶¶ 6 n.1, 46, 47; *see also Clapper*, 568 U.S. at 409 (“Allegations of *possible* future injury are not sufficient.”).

Several other district courts have similarly found that the theft of non-sensitive data, absent any other allegation that the feared harms of identity theft have materialized, falls short of the “imminent” threshold. *See, e.g., Kylie S. v. Pearson PLC*, 475 F. Supp.3d 841, 848 (N.D. Ill. 2020) (“In short, Plaintiffs’ theory fails because the disclosed data [names, emails, and birthdays] is not sensitive enough to materially increase the risk of identity theft.”); *Fus v. CafePress, Inc.*, No. 19-cv-06601, 2020 WL 7027653, at *3 (N.D. Ill. Nov. 30, 2020) (“[M]ost of Fus’s information possessed by CafePress at the time of the hack was publicly available information, such as his billing and shipping address and personal email address. However, the disclosure of such information does not expose Fus to a significant risk of identity theft or fraud.”); *In re Vtech Data Breach Litig.*, No. 15 C 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) (“Plaintiffs have not shown an increased risk of identity theft due to a data breach because they do not allege how the stolen data would aid identity thieves in their efforts.”); *Cooper v. Bonobos, Inc.*, No. 20-CV-854 (JMF), 2022 WL 170622, at *5 (“Put simply, given the nature and age of the data, the

likelihood that its exposure would result in harm to Cooper is too remote to support standing.”); *De Medicis v. Ally Bank*, 2022 WL 3043669, at *10 (S.D.N.Y. Aug. 2, 2022) (“Instead, as alleged, Plaintiff’s username and password appears to be less sensitive information ‘that can be rendered useless to cybercriminals and does not pose the same risk of future identity theft or fraud to plaintiffs if exposed.’”) (quoting *McMorris v. Carlos Lopez & Assoc.*, 995 F.3d 295, 302 (2d Cir. 2021)). In each of these cases, the court dismissed the plaintiffs’ claims for lack of standing, and this Court follows suit.

B. Mitigation-related and Emotional Distress Injuries

Plaintiffs also argue that the “identifiable trifle” of time they expended in response to the data breach constitutes a sufficiently concrete injury to support standing. [20] at 8 (quoting *Craftwood II, Inc. v. Generac Power Sys., Inc.*, 920 F.3d 479, 481 (7th Cir. 2019)). In their complaint, Plaintiffs allege that they spent time monitoring for and removing unwanted spam and phishing emails, spent time contacting Defendants about the data breach, and, in the case of Plaintiff Jun, spent time filing a proactive police report. [1] ¶¶ 8, 9, 14, 15, 37, 66, 79, 100, 115.

But “mitigation expenses qualify as ‘actual injuries’ only when the harm is imminent,” *Lewert*, 819 F.3d at 967, and “plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 568 U.S. at 416. In *Craftwood II*, the Seventh Circuit held that the plaintiffs’ time and mitigation expenses spent dealing with unwanted faxes sent by defendant in violation of the Telephone

Consumer Protection Act was sufficiently concrete for Article III standing because the harm had already occurred—the plaintiffs had already received the unwanted faxes from the defendant. *See Craftwood II* 920 F.3d at 481. Similarly, in *Remijas* and in *Lewert*, the Seventh Circuit held that the plaintiffs’ mitigation expenses in response to the theft of their credit card information was sufficient to confer Article III standing because the harm they feared—fraudulent charges on their credit card—was sufficiently imminent and for some of the plaintiffs, had already occurred. *Remijas*, 794 F.3d at 693; *Lewert*, 819 F.3d at 967.

Unlike the plaintiffs in *Craftwood II*, *Remijas*, and *Lewert*, however, Plaintiffs’ fears here rely on “speculation about the ‘unfettered choices made by independent actors not before the court.’” *Clapper*, 568 U.S. at 414 n.5 (quoting *Lujan*, 504 U.S. at 562)). The data breach disclosed Plaintiffs’ non-sensitive information (their email addresses, phone numbers, and delivery addresses), and none of the Plaintiffs had their identities stolen or became the victim of a phishing scam. As the complaint contains no allegation indicating that the Plaintiffs’ feared harms are certainly impending, they cannot rely on their time and money spent in response to fears that are too speculative to support standing under Article III. *See Clapper*, 568 U.S. at 416 (“If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.”).

Similarly, Plaintiffs’ allegations that they experienced mental aggravation, anxiety, and emotional distress from the data breach, [1] ¶¶ 37, 66, 79, 100, 115, also

remain insufficient to provide standing under Article III, as such emotional injuries constitute “quintessential abstract harms that are beyond” the Court’s power to remedy. *Wadsworth v. Kross, Lieberman & Stone, Inc.*, 12 F.4th 665, 668 (7th Cir. 2021). Indeed, if these emotional injuries alone were sufficient to invoke the jurisdiction of federal courts, “then everyone would have standing to litigate about everything.” *Id.*

C. Loss of Privacy

Plaintiffs also argue that the theft of their personal information—email addresses, phone numbers, and delivery addresses—suffices to confer standing under Article III. [20] at 7.

As an initial matter, Plaintiffs do not allege in their complaint that they had a property or privacy interest in their email addresses, phone numbers, and delivery addresses. And such allegations may not help, as the Seventh Circuit has expressed skepticism towards such a claim, even where the personal information stolen in the data breach was decidedly more sensitive than the information at issue here. *See Remijas*, 794 F.3d at 695 (noting that the theft of plaintiffs’ credit card information is an “abstract injury” insufficient to confer standing “particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.”); *Lewert*, 819 F.3d at 968 (noting the lack of authority in support of plaintiffs’ argument that they have a property right to their credit card data and that the theft of that data “supports standing just as well as the theft of one’s car would.”).

Several other federal courts have similarly rejected the argument that a loss of privacy arising from the theft of non-sensitive personal information, standing alone, supports Article III standing. *See, e.g., In re Practicefirst Data Breach Litigation*, 2022 WL 354544 (W.D.N.Y. Feb. 2, 2022) (collecting cases); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp.3d 524, 533 (D. Md. 2016) (“Second, Khan argues that the data breach has caused a loss of privacy that constitutes an injury in fact. However, she has not identified any potential damages arising from such a loss and thus fails to allege a ‘concrete and particularized injury.’”); *In re Zappos.com, Inc.*, 108 F. Supp.3d 949, 962 n.5 (D. Nev. 2015) (“Even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury.”); *C.C. v. Med-Data Incorporated*, No. 21-2301-DDC-GEB, 2022 WL 970862, at *10 (D. Kan. Mar. 31, 2022) (“In sum, plaintiff’s standing problem here is a familiar one: she hasn’t alleged any concrete or particularized harm from her alleged loss of privacy. Her loss of privacy, in and of itself, is not a concrete harm that can provide the basis for Article III standing.”); *I.C. v. Zynga, Inc.*, 20-cv-01539-YGR, 2022 WL 2252636, at *8 (N.D. Cal. April 29, 2022) (“[I]n data breach cases, courts must examine the nature of the specific information at issue to determine whether privacy interests are implicated at all.”).

Nevertheless, the Supreme Court has recognized that certain intangible injuries can be sufficiently concrete for purposes of Article III standing. *See Spokeo, Inc.*, 578 U.S. at 341. To determine if an alleged intangible injury is sufficiently concrete to confer standing, the Court looks to history and the judgment of Congress.

Id. In looking to history, the Court must determine if the alleged injury bears “a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American Courts.” *Spokeo, Inc.*, 578 U.S. at 341. The Court finds that the closest analog to the Plaintiffs’ claims is the tort of publicity to private life, because Plaintiffs allege that McDonald’s negligence led to the disclosure of Plaintiffs’ personal information. [1] ¶¶ 100, 115. But liability may not be imposed for this tort if the disclosure would not be “highly offensive to a reasonable person,” or if the information is already publicly known. Restatement (Second) of Torts § 652D, cmt. b (Am. L. Inst. 1977) (“There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public.”).

Here, Plaintiffs do not allege that they considered their email addresses, phone numbers, and delivery addresses to be private or otherwise sensitive or confidential. And the disclosure of the type of information at issue here—by its very nature—would not be highly offensive to a reasonable person. Thus the mere disclosure of the type of information at issue here does not confer standing under Article III. Nor have Plaintiffs identified any federal statute conferring a right of privacy or any other interest in their email addresses, phone numbers, or delivery addresses.

D. Statutory Violations as an Injury-in-Fact

Finally, Plaintiffs allege that Defendants’ retention of Plaintiff Jun’s data, which continued after Jun had ceased using the McDelivery app, violated the Republic of Korea’s Personal Information Privacy Act. [1] ¶ 78, 99–100, 107–08, 130–32. Plaintiffs allege that this violation “works a concrete and particularized Article

III injury.” [20] at 7 (quoting *Cothron v. White Castle Sys.*, 20 F.4th 1156, 1161 (7th Cir. 2021)).

The Court need not decide whether Defendants’ conduct violated Korea’s PIPA, because, even if it did, bare procedural violations of a statute, absent any concrete harm, remain insufficient to support Article III standing. *See Spokeo, Inc.*, 578 U.S. at 341 (“Article III standing requires a concrete injury even in the context of a statutory violation.”); *Meyers v. Nicolet Restaurant of De Pere, LLC*, 843 F.3d 724, 727 n.2 (7th Cir. 2016) (“A violation of a statute that causes no harm does not trigger a federal case.”). Here, the complaint contains no allegation explaining how Defendants’ retention of Plaintiff Jun’s data caused him any concrete injury.

Plaintiffs’ reliance on *Cothron v. White Castle Sys.* is misplaced because *Cothron* involved the dissemination of an individual’s biometric data without their informed consent in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/ *et seq.* 20 F.4th 1156, 1161 (7th Cir. 2021). In the context of BIPA, the Seventh Circuit has recognized that the collection of an individual’s biometric data without his informed consent would be “an invasion of his private domain, much like an act of trespass would be” because “each individual person has distinct biometric identifiers.” *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020). In *Fox v. Dakota Integrated Sys., LLC*, the court reasoned that “an unlawful *retention* of a person’s biometric data is as concrete and particularized an injury as an unlawful *collection* of a person’s biometric data.” *Fox v. Dakota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020). But this case is not about biometric data.


See Fox, 980 F.3d 1146, 1155 & n2 (noting that an individual’s address, date of birth, telephone number, credit card and social security number are “meaningfully different” from biometric information like retinal or iris scans, facial geometry, fingerprints, or handprints, which are “immutable, and once compromised, are compromised forever.”). And without some allegation that Jun suffered a concrete injury from Defendants’ wrongful retention of his personal information, Jun has just the bare procedural violation of PIPA, which will not suffice to confer standing under Article III.

IV. Conclusion

For the reasons explained above, the Court finds that Plaintiffs lack Article III standing to pursue their claims. Having so found, the Court need not consider whether Plaintiffs’ complaint would also fail under Rule 12(b)(6). The Court grants Defendants’ motion to dismiss [18] and dismisses the complaint without prejudice for lack of jurisdiction. To the extent Plaintiffs can, consistent with their obligations under Rule 11, amend the complaint to allege Article III standing, they may file an amended complaint by October 24, 2022.

Dated: September 27, 2022

Entered:


John Robert Blakey
United States District Judge