
IN THE
APPELLATE COURT OF ILLINOIS
FIRST DISTRICT

TERRY KIMBER and VERONICA MARTIN,	)	Appeal from the
	)	Circuit Court of
Plaintiffs-Appellants,	)	Cook County, Chancery
	)	Division.
v.	)	
	)	No. 2023CH09293
COOK COUNTY HEALTH AND HOSPITALS	)	
SYSTEM and PERRY JOHNSON & ASSOCIATES,	)	
INC.,	)	Honorable
	)	Caroline K. Moreland,
Defendants-Appellees.	)	Judge, presiding.

JUSTICE PUCINSKI delivered the judgment of the court, with opinion.
Justices Hyman and Evans concurred in the judgment and opinion.

OPINION

¶ 1 Plaintiffs filed a class action lawsuit against Cook County Health and Hospitals System (CCH) and Perry Johnson & Associates, Inc. (PJA), following an April 2023 data breach of PJA's systems, which compromised personally identifying information (PII) and personal health information (PHI) that CCH had collected from plaintiffs. Plaintiffs bring claims of negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, unjust

enrichment, and violations of the Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/1 *et seq.* (West 2024)).

¶ 2 Plaintiffs, Terry Kimber and Veronica Martin, maintain that the data breach exposes them to an increased risk of identity theft or fraud. Martin alleges that she has also suffered from an increase in spam calls, texts, and e-mails as a result of the breach. Apart from Martin’s spam allegation, however, neither plaintiff alleges fraudulent or unauthorized use of their data.

¶ 3 On defendants’ motions to dismiss under section 2-619.1 of the Code of Civil Procedure (735 ILCS 5/2-619.1 (West 2024)), the trial court dismissed the action with prejudice for lack of standing, finding the alleged harms to be “speculative and conclusory, not imminent and substantial.” Plaintiffs appealed.

¶ 4 Because plaintiffs failed to establish an actual injury or an imminently impending injury and because the allegations of spam are not fairly traceable to the data breach, we affirm the trial court’s ruling that plaintiffs lacked standing.

¶ 5 I. BACKGROUND

¶ 6 Defendant CCH maintains two hospitals and numerous other healthcare facilities in Cook County. In the course of its business, CCH collects PII and PHI from its patients. Plaintiffs allege that CCH required patients to provide this information as a condition of receiving health care services. Defendant PJA provides medical transcription services to CCH, which entailed PJA receiving and maintaining certain patient information.

¶ 7 Between approximately March 27 and May 2, 2023, an unauthorized third party accessed PJA files containing the private information of 1.2 million CCH patients. The “affected protected health information may have included names, and some combination of *** dates of birth, addresses, medical record numbers, encounter numbers, medical information, and

dates/times of service.” The files also contained the Social Security numbers of approximately 2,600 people.

¶ 8 On November 2, 2023, CCH sent letters out to some of its patients, informing them that their private information “may have been affected.” On November 7, 2023, Kimber filed a putative class action lawsuit against appellees. After Martin filed a similar suit, plaintiffs consolidated the suits and filed an amended complaint.

¶ 9 The amended complaint sets forth a litany of injuries resulting from the data breach. Both plaintiffs claim that they (i) are exposed to a substantial and imminent risk of identity theft and medical identity theft, (ii) have suffered a loss of the market value of their PII/PHI because it is no longer confidential and may be sold or purchased by criminal actors, (iii) have suffered privacy violations through the disclosure of confidential, sensitive information, (iv) have been injured by overpayment of services to CCH that did not include adequate data security, and (v) have incurred time and opportunity costs in mitigating the consequences of the data breach. Martin makes the additional allegation that she has (vi) experienced an increase in spam calls, texts, and e-mails following the breach. Plaintiffs request monetary damages and equitable relief.

¶ 10 Defendants filed separate motions to dismiss pursuant to section 2-619.1 of Code of Civil Procedure (*id.*). They first argued that plaintiffs had not pled a cognizable injury and thus lacked standing. Defendants also argued that the claims were insufficiently or defectively pled under section 2-615 (*id.* § 2-615). While the motions were pending, our supreme court filed *Petta v. Christie Business Holdings Co., P.C.*, 2025 IL 130337, which addressed standing in the context of a breach of a medical entity’s e-mail servers. The parties submitted supplemental briefs discussing *Petta* to the trial court.

¶ 11 Finding that plaintiffs had failed to allege actual injuries and that their allegations concerning the risk of future injuries were speculative and conclusory rather than imminent and substantial, the circuit court dismissed the complaint with prejudice. Plaintiffs appealed.

¶ 12 II. ANALYSIS

¶ 13 A. Standard

¶ 14 A party may bring a combined section 2-615 and 2-619 motion to dismiss under section 2-619.1 of the Code of Civil Procedure. See 735 ILCS 5/2-615, 2-619, 2-619.1 (West 2024). Combined motions separately attack the sufficiency of the allegations set forth in the complaint and present affirmative defenses that defeat the claim even if the allegations are deemed true. A challenge to a plaintiff's standing to bring a claim may be raised under section 2-619(a)(9) (*id.* § 2-619(a)(9)). Because the trial court ruled solely on plaintiffs' standing and because we find the lack of standing to be dispositive on appeal, we limit our discussion to the standing issue.

¶ 15 “‘[L]ack of standing is an affirmative defense, which is the defendant's burden to plead and prove.’ ” *Fausett v. Walgreen Co.*, 2025 IL 131444, ¶ 46 (quoting *Lebron v. Gottlieb Memorial Hospital*, 237 Ill. 2d 217, 252 (2010)). “The function of the doctrine of standing is to insure that issues are raised only by those parties with a real interest in the outcome of the controversy.” *Wexler v. Wirtz Corp.*, 211 Ill. 2d 18, 23 (2004). The doctrine also serves to limit court dockets to “only those disputes which are truly adversarial and capable of resolution by judicial decision.” *Greer v. Illinois Housing Development Authority*, 122 Ill. 2d 462, 488 (1988).

¶ 16 Although standing is not a jurisdictional issue in Illinois as it is in federal courts (see, *e.g.*, *Fausett*, 2025 IL 131444, ¶ 36 (distinguishing state standing against article III standing under

the United States Constitution (U.S. Const., art. III))), the requirement of standing serves a similar purpose of preserving court attention and intervention to only those disputes appropriate for judicial review. Limits to standing ensure that courts are deciding “ ‘actual, specific controversies, and not abstract questions or moot issues.’ ” *Davis v. Yenchko*, 2024 IL 129751, ¶ 17 (quoting *In re Marriage of Rodriguez*, 131 Ill. 2d 273, 279-80 (1989)).

¶ 17 We do not follow federal standing law, but given the similar guiding principles, Illinois courts may treat federal case law as instructive. See, e.g., *Maglio v. Advocate Health & Hospitals Corp.*, 2015 IL App (2d) 140782, ¶ 25; cf. *Petta*, 2025 IL 130337, ¶ 21 (analyzing standing issue with reference to *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021)).

¶ 18 In Illinois, standing “requires only some injury in fact to a legally cognizable interest.” *Greer*, 122 Ill. 2d at 492 (citing *Glazewski v. Coronet Insurance Co.*, 108 Ill. 2d 243 (1985)). “ ‘[T]he claimed injury, whether “actual or threatened” [citation], must be: (1) “distinct and palpable” [citation]; (2) “fairly traceable” to the defendant’s actions [citation]; and (3) substantially likely to be prevented or redressed by the grant of the requested relief [citations].’ ” *Petta*, 2025 IL 130337, ¶ 18 (quoting *Greer*, 122 Ill. 2d at 492-93). Standing does not require that an injury already occurred; a plaintiff may allege “a concrete injury in fact based on an *imminent, a certainly impending, or a substantial risk* *** and a concrete harm caused by exposure to this risk.” (Emphasis added.) *Olson v. Ferrara Candy Co.*, 2025 IL App (1st) 241126, ¶ 27, *appeal denied*, No. 132021 (Ill. Nov. 26, 2025). “ ‘[A]llegations of *possible* future injury’ are not sufficient.” (Internal quotation marks omitted and emphasis in original.) *Maglio*, 2015 IL App (2d) 140782, ¶ 25) (quoting *Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013)).

¶ 19 A section 2-619 motion “admits well-pleaded facts but does not admit conclusions of law and conclusory factual allegations unsupported by allegations of specific facts alleged in the complaint.” *McIntosh v. Walgreens Boots Alliance, Inc.*, 2019 IL 123626, ¶ 16. On review of a section 2-619(a)(9) motion, we determine whether there exists a genuine issue of material fact that should have precluded the dismissal and whether the dismissal was proper as a matter of law. *Better Government Ass’n v. Illinois High School Ass’n*, 2017 IL 121124, ¶ 21. “[U]nsupported conclusions, opinions, or speculation are insufficient to raise a genuine issue of material fact.” *Colon v. Illinois Central R.R. Co.*, 2024 IL App (1st) 221841, ¶ 27.

¶ 20 “Where a plaintiff lacks standing, the proceedings must be dismissed because the lack of standing negates the plaintiff’s cause of action.” *Maglio*, 2015 IL App (2d) 140782, ¶ 20 (citing *Wexler*, 211 Ill. 2d at 22). Standing is a question of law, so we review the issue *de novo*. *Fausett*, 2025 IL 131444, ¶ 33.

¶ 21 B. Plaintiffs Lack an Injury in Fact to a Legally Cognizable Interest

¶ 22 Plaintiffs have pled several injuries including (i) a risk of future identity theft or fraud, (ii) an increase in spam, (iii) the time and money costs of mitigating potential injuries, (iv) the diminution of the market value of their personal information, and (v) overpayment of services to CCH. We consider each injury in turn.

¶ 23 1. The Risk of Future Identity Theft or Fraud Is Speculative and Not Imminent

¶ 24 Although plaintiffs have not pled that they have suffered any specific fraudulent activity connected to the data breach, plaintiffs maintain that the breach exposes them to a “substantial and imminent risk of identity theft and medical identity theft.” The complaint, as well as the briefs, outline a variety of ways in which PII/PHI may be exploited by criminal actors. For instance, the data could be “aggregated” with other information and sold on black markets. See

Flores v. Aon Corp., 2023 IL App (1st) 230140, ¶ 16 (“[D]ata thieves can compile ‘Fullz’ packages” combining compromised data with other available data “that can be sold to third parties to be later used for illegal purposes.”). Criminals may use the data to commit fraud or to extort payment from the patient by threatening disclosure of private information. And fraudulent activity may have downstream effects on the victims’ credit score, their ability to acquire loans, or their access to medical care. Plaintiffs argue that PII and especially PHI are targeted by hackers for its value, thus the breach substantially increases the risk that they will be victimized by criminal exploitation of their data.

¶ 25 Both plaintiffs argue that the data breach alone exposes them to a heightened risk of identity theft or fraud sufficient to establish the existence of an imminent or substantial threatened injury for standing purposes. Although Martin makes an additional allegation that she has already experienced an increase in spam, because we find that injury is not “fairly traceable” to the data breach (see ¶¶ 41-52 *supra*) we consider it irrelevant to our future injury analysis. Thus, for the purposes of our future injury analysis, we do not distinguish the plaintiffs. Ultimately, we find that the allegations fail to establish a substantial, imminent threatened injury sufficient to confer standing.

¶ 26 To have standing, plaintiff must have suffered a “concrete” injury or face an “imminent,” “certainly impending,” or “substantial risk of harm” as a consequence of the wrongful conduct. *Olson*, 2025 IL App (1st) 241126, ¶ 25. Allegations that plaintiffs face only an “increased *risk*” of identity theft or fraud as a result of data exposure are insufficient. (Emphasis added.) *Petta*, 2025 IL 130337, ¶ 21; see *Maglio*, 2015 IL App (2d) 140782, ¶ 24 (claims of risk were speculative because “no such identity theft has occurred to any of the plaintiffs”). “[A]n increased risk or credible threat of impending harm is plainly different from *certainly*

impending harm.” (Internal quotation marks omitted, emphasis added, and emphases omitted.)
Maglio, 2015 IL App (2d) 140782, ¶ 26 (analogizing federal standing case law).

¶ 27 *Olson* presents three considerations for determining whether a prospective injury is imminent: (1) “whether the PII was exposed as the result of a targeted attempt to obtain that data,” (2) “whether any portion of the stolen or accessed PII has already been misused,” and (3) “whether the PII at issue is sensitive, such that there is a high risk of identity theft or fraud.” *Olson*, 2025 IL App (1st) 241126, ¶ 28.

¶ 28 Illinois courts treat the second factor as determinative. Each of the Illinois courts addressing standing based on a future injury in the context of a data breach only found standing where there was an actual or attempted misuse of the exposed data that was fairly traceable to the breach. In *Petta* and *Maglio*, the supreme court and appellate court respectively held that the potential of a future injury was speculative and did not confer standing. See *Petta*, 2025 IL 130337, ¶ 21; *Maglio*, 2015 IL App (2d) 140782, ¶ 29 (the fact that two plaintiffs in a class of four million had received notice of fraudulent activity “does not show that plaintiffs here face imminent, certainly impending, or a substantial risk of harm *** where no such activity has occurred with respect to their personal data”). In comparison, the courts in *Olson* and *Flores* found the risk of future misuse of plaintiffs’ data to be “imminent and substantial” where certain plaintiffs in either case had experienced fraudulent charges that the courts determined were fairly traceable to the data breach. See *Flores*, 2023 IL App (1st) 230140, ¶ 15 (two plaintiffs had experienced fraudulent charge attempts, and others complained of increased spam); *Olson*, 2025 IL App (1st) 241126, ¶¶ 30-32. For *Olson* and *Flores*, the existence of fraudulent activity for certain plaintiffs was sufficient to demonstrate an imminent risk of future injury to plaintiffs who had not been subjected to attempted fraud yet.

¶ 29 We take the presence or absence of attempted fraud to be the critical factor. The presence of attempted fraud conferred standing in *Flores* and *Olson* but was absent in the cases finding no standing (*Maglio* and *Petta*). In this case, neither Kimber nor Martin has pled that they were victim to any attempted fraud related to the breach. Thus, we find that this case follows the course of *Maglio* and *Petta*; the unmaterialized speculation of future identity theft does not confer standing.

¶ 30 Considering the other two factors set forth by *Olson*, though these tend to support plaintiffs' argument that there is an increased risk of their data being misused in the future, the risk of that injury remains too speculative and insufficiently imminent to confer standing.

¶ 31 *Olson*'s second factor considers the sensitivity and the value of the data. Plaintiffs have alleged in their complaint that the compromised data—including Social Security numbers, medical information, names, and dates of birth—are private, sensitive, and exploitable by criminals. Among other things, plaintiffs note that the data may be sold on its own, may be compiled with other public information to be sold or put to fraudulent purposes, or may even be the basis for extortion attempts. The value of this information is obvious as has been generally acknowledged by state and federal courts. See, *e.g.*, *Olson*, 2025 IL App (1st) 241126, ¶¶ 28-29.

¶ 32 The third factor is whether the plaintiffs' data was collected in a "targeted attempt" to obtain their data. It stands to reason that the risks attendant to incidental data exposure (*e.g.*, the erroneous publication of confidential information) are different compared to an intentional theft of specific data.

¶ 33 Plaintiffs emphasize this factor to draw a distinction between *Maglio* and *Petta* on the one hand and *Flores* and *Olson* on the other. The exposure of the plaintiffs' data in *Maglio* and

Petta was incidental to other criminal activity, whereas *Flores* and *Olson* involved targeted attempts to obtain data.

¶ 34 In *Maglio*, four physical computers were stolen from the defendant’s office, and those unencrypted computers contained plaintiffs’ sensitive information (*e.g.*, medical data, Social Security numbers, etc.). *Maglio*, 2015 IL App (2d) 140782, ¶ 5. As plaintiffs argue, the criminals targeted the *computers*, not the data; there was no allegation that the data on the computers was ever improperly accessed. The target of the theft may have been the independently valuable computer hardware.

¶ 35 In *Petta*, there was unauthorized access to one of the defendant’s business e-mail accounts that may have contained plaintiff’s personal information. *Petta*, 2025 IL 130337, ¶¶ 5-6. An independent investigation determined that “the unauthorized third party was attempting to intercept a financial transaction, not steal patients’ private personal information.” *Id.* ¶ 20. The plaintiff’s data may have been exposed, but the facts suggested that it was not the target of the attack.

¶ 36 In comparison, *Flores* and *Olson* involved what might be characterized as targeted data breaches. In each case, the defendant entities gave notice to the plaintiffs that there was unauthorized access to their network or systems containing their sensitive data. From the allegations and the contexts of the breaches, it appears as though the third parties intended to access the data. See *Olson*, 2025 IL App (1st) 241126, ¶ 29 (“data breach was the result of an attack by thieves who *** stole the plaintiffs’ PII over a seven-day period”); *Flores*, 2023 IL App (1st) 230140, ¶¶ 3, 5 (third party repeatedly accessed defendant’s systems that contained sensitive information). Because the nature of the data breach in this case is more similar to *Olson* and *Flores*, plaintiffs recommend that we follow their course and find standing,

¶ 37 Plaintiffs insist that a court may infer that an injury is imminent where a plaintiff's sensitive information is exposed in a targeted data breach. Courts have observed that, for targeted data breaches, "it is reasonable to assume that the data thieves will use the stolen data for fraudulent purposes." *Id.* ¶ 16 (citing *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 388 (6th Cir. 2016)). Plaintiffs argue that we should infer an imminent criminal intent to use the exposed data for fraudulent purposes based on the circumstances of PJA's data breach. Their argument is supplemented by allegations in the complaint setting forth general information about the value of the categories of the underlying data, examples of how criminals may misuse such data, and how such misuses may injure the plaintiffs.

¶ 38 Reading these allegations in the light most favorable to the plaintiffs, the allegations only set forth an increased risk of identity theft or fraud, not an imminent injury. Plaintiffs' allegations amount to circumstantial speculation about the intent of the third parties, the data that was obtained, the prospective criminal use of such information, and the impact on the plaintiffs. Reading the allegations in plaintiffs' favor, we cannot say that plaintiffs are exposed to an imminent or certainly impending injury. Whereas we agree that plaintiffs are exposed to a higher risk of identity theft as a result of the breach, an increase in risk is not sufficient to confer standing. *Petta*, 2025 IL 130337, ¶ 21. We are skeptical of the imminence of an injury that requires us to rely on speculation about an unknown third party's intent or motivations. Considering other allegations in the complaint, the likelihood of an imminent injury as to these plaintiffs is more attenuated: the notices of the data breach only advised that the unauthorized party acquired copies of "certain files" and that CCH's patients "may" be affected; and the described fraudulent uses of the data are only speculative possibilities.

¶ 39 As we have stated, we believe the presence of a traceable misuse of the compromised data is determinative in this analysis. No traceable misuse is presented in this case, and we find plaintiffs’ allegations about potential misuse to be too speculative to confer standing.

¶ 40 Our ruling on this issue also forecloses the injunctive and declaratory relief requested by the complaint regarding defendants’ current data practices. See *Davis*, 2024 IL 129751, ¶¶ 23-24 (injunctive relief denied where future injury was speculative). Plaintiffs’ requests for equitable relief are predicated on the same speculated injuries discussed in this section, and we do not analyze the standing for that relief differently.

¶ 41 2. Martin’s Alleged Increased Exposure to Spam Is Conclusory and Not Fairly Traceable
to the CCH/PJA Data Breach

¶ 42 Martin maintains that her increased receipt of spam texts, calls, and e-mails constitutes a concrete and cognizable injury. Whereas we find it conceivable that spam could constitute a concrete injury for the purposes of standing (see *Flores*, 2023 IL App (1st) 230140, ¶ 15), we find that, under *Petta*, the increased spam is not fairly traceable to the data breach.

¶ 43 We begin our discussion by noting that Martin’s allegation of increased spam is conclusory. Martin claims she has “suffered from an increase in spam call [*sic*], texts, and e-mails as a result of her PII/PHI being compromised in the [d]ata [b]reach.” Apart from the unstated but implied timing of the spam, there are no supporting facts tracing the spam to the data breach. The causation is pled in a conclusory fashion. There are no allegations, for instance, that the spam contained information exposed in the breach, made reference to her health information or CCH/PJA, or otherwise suggested some relationship to the breach.

¶ 44 Additionally, plaintiff has not pled that her contact information was exposed in the breach. Nor does she allege that her phone number and e-mail could only have been obtained through the data breach.

¶ 45 Based on the record before us, we agree that the increased spam is not fairly traceable to the data breach under *Petta*.

¶ 46 In *Petta*, defendant, a medical services provider, notified the plaintiff that her data (including her Social Security number and medical insurance information) may have been compromised due to unauthorized access to defendant’s business e-mail account. *Petta*, 2025 IL 130337, ¶¶ 5-6. Whereas the data breach notice explained that the unauthorized access was done by a third party attempting to intercept a financial transaction, it was not known whether the plaintiff’s data in the compromised account was accessed or obtained. *Id.* Sometime after the breach, Petta claimed that an unauthorized loan application was made using her information, including her “ ‘phone number, city, and state,’ ” and that she received numerous calls regarding the application. *Id.* ¶ 9. Petta sued the provider, asserting that the breach had exposed her to a heightened risk of identity fraud and tracing the unauthorized loan application to the data breach. *Id.* ¶¶ 8-9.

¶ 47 The supreme court held that the fraudulent loan application was not traceable to the breach because the information used in the loan application consisted of public information that “could be found in a publicly available phone directory” and not any of the specific information exposed by the breach. *Id.* ¶¶ 24-25. Thus, the court affirmed that Petta lacked standing to pursue her claim against the provider. *Id.* ¶ 27.

¶ 48 The same distinction applies here. Plaintiffs allege that CCH and PJA committed a wrongful act where they failed to adequately protect sensitive PII and PHI. But Martin does

not allege that any of the sensitive information compromised by the breach was used or included in the spam. The only inference we can make from the bare allegation is that the spammers made use of Martin’s phone number(s) and e-mail address(es), data that Martin’s original complaint characterized as “unregulated data available elsewhere,” *i.e.*, outside of the compromised data. Because the spam did not use or concern the exposed data, the spam cannot be said to be fairly traceable to the data breach. The timing of the spam alone is insufficient to trace it back to the data breach in the absence of any other facts.

¶ 49 Plaintiffs rely on *Olson* and *Flores* to urge the opposite conclusion, arguing that both cases found that increases in spam were fairly traceable to a data breach where the plaintiff also alleges that the captured information may be compiled with publicly available information in “Fullz” packages that are resold and exploited for illegal purposes. We find both *Olson* and *Flores* to be distinguishable because, in each case, at least one other plaintiff had pled a specific misuse of nonpublic personal information exposed in the data breach.

¶ 50 In *Flores*, following a data breach of the defendant’s systems, plaintiff Williams pled that someone attempted to process an unauthorized \$499.99 charge to her PayPal account after the breach, and plaintiff Dube alleged that she was charged for a prescription that she did not order. *Flores*, 2023 IL App (1st) 230140, ¶ 7. The appellate court found that these fraudulent charges were fairly traceable to the data breach because “Williams and Dube alleged that defendant informed both plaintiffs that their ‘benefit enrollment information’ was obtained during the data breach” and “it is possible that it included Williams’s and Dube’s payment information.” *Id.* ¶ 16. Similarly, in *Olson*, plaintiff Wesson suffered an unauthorized charge to his credit union account two months after his employer suffered a data breach. *Olson*, 2025 IL App (1st) 241126, ¶ 11. Although the defendant submitted a declaration that it never had information

concerning Wesson’s credit union account, the appellate court found that the fraudulent charge was nonetheless fairly traceable to the breach given the timing, the fact that information exposed in the breach could have been combined with other available information to commit the fraud, and that Wesson asserted that he was not aware of any other data breaches of his PII that would explain the attempted charge. *Id.* ¶¶ 32-34. In both *Flores* and *Olson* there were specific examples of attempted misuse of data involved in the breach.

¶ 51 It is true that the *Flores* and *Olson* courts also found standing for plaintiffs in the suits who alleged only an exposure of their data and an increase in spam and targeted marketing. However, each case only analyzed traceability with respect to the fraudulent charges. The courts apparently extended those traceability findings to the spam allegations. We do not disagree with the logic of that extension; a finding that fraudulent charges were traceable to a data breach lends credibility to the suggestion that spam experienced by other victims of the data breach shared the same cause. And the presence of specific attempts at fraud involving the compromised data also suggests an imminent or substantial risk of the exploitation of the other plaintiffs’ data.

¶ 52 In this case, however, there are no such indications that the data compromised by the breach is being misused. Martin does not allege that her contact information was exposed by the data breach, and even if it was, she has conceded that the data was “unregulated” and “available elsewhere.” Martin does not allege that the substance of the spam suggested a connection to the breach. All that Martin offers is the bare and conclusory allegation that she has suffered an increase in spam caused by the breach. Based on the pleadings, the alleged spam is not fairly traceable to defendant; the connection is only speculative.

¶ 53 3. Time Spent Mitigating Potential Injuries Is Not a Cognizable Injury Unless the Injury Is Substantial and Imminent

¶ 54 In response to the notice that their data had been compromised, plaintiffs generically allege that they made reasonable efforts to mitigate the impact of the breach, incurring a time and monetary cost. Plaintiffs argue that the costs they incurred to mitigate their exposure constitutes an injury-in-fact that can confer standing. Setting aside that the complaint is bereft of supporting facts indicating what efforts were undertaken, efforts to mitigate a future injury will not confer standing unless the prospective injury is imminent and substantial. See *Petta v. Christie Business Holding Co., P.C.*, 2023 IL App (5th) 220742, ¶ 25, (out-of-pocket expenses and time and energy spent monitoring accounts did not support standing in response to a speculative threat), *aff'd*, 2025 IL 130337; see *Clapper*, 568 U.S. at 416 (Litigants cannot “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.”); *cf. Olson*, 2025 IL App (1st) 241126, ¶ 42 (“[L]ost time Olson and Wesson spent monitoring their accounts *** is not a self-inflicted harm arising from a mere subjective fear of injury” where “the stolen PII has allegedly already been misused.”).

¶ 55 Allegations of time and effort spent mitigating a future harm may not confer standing unless that future injury is substantial and imminent. Because we have found that the risk of identity fraud is speculative and not imminent, the time and effort spent mitigating those risks do not confer standing.

¶ 56 4. Diminished Value in Plaintiffs' Private Information Does Not Confer Standing

¶ 57 Plaintiffs also allege that they have suffered an injury in the diminution of the value of their PII. As they allege, “PII/PHI is a valuable property right” whose value is measurable as a

commodity. They allege that American companies spend billions of dollars annually to collect consumer data and that criminal markets exist for criminals to trade stolen PII/PHI. Per plaintiffs, dossiers of PII/PHI may be sold for up to \$1,300 on black markets. As a consequence of the data breach, plaintiffs argue that they have been deprived of the value of their PII/PHI. Plaintiffs claim that this lost value constitutes an injury-in-fact.

¶ 58 We reject this argument for a number of reasons. First, personal information has not been recognized as a property right in Illinois courts. See *Petta*, 2023 IL App (5th) 220742, ¶ 17 (“This court is unaware of any case law holding that a person has a property right in [their] personal information. The federal courts have refrained from finding such a right, and we decline to create one.”).

¶ 59 We also question whether it is the court’s prerogative to confer standing for what amounts to an informational injury where our state’s statutory scheme does not acknowledge such an injury. Compare the Biometric Information Privacy Act (Biometric Privacy Act) (740 ILCS 14/1 *et seq.* (West 2024)) and the Genetic Information Privacy Act (410 ILCS 513/1 *et seq.* (West 2024)) with the Personal Information Protection Act (815 ILCS 530/1 *et seq.*) (West 2024).¹ The General Assembly has created special statutory standing for injuries involving certain types of private information, such as biometric information. See *Fausett*, 2025 IL 131444, ¶¶ 39-41; see also *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 33 (under the Biometric Privacy Act, a plaintiff has standing to sue for a violation of the act without establishing an actual injury). The statutory scheme does not appear to extend the same special standing rules to the types of information at issue in this case.

¹Plaintiffs allege violations of the Personal Information Protection Act as part of their *per se* negligence and Consumer Fraud and Deceptive Business Practices Act claims.

¶ 60 The Personal Information Protection Act regulates how entities secure and manage personal information, including the data at issue in this case (*i.e.*, Social Security numbers, State identification card numbers, and financial and medical information). 815 ILCS 530/5(1) (West 2024). The Personal Information Protection Act also regulates how entities give notice of data breaches. *Id.* § 10(c). The Personal Information Protection Act does not specifically provide for an independent cause of action, but “[a] violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.” *Id.* § 20.

¶ 61 Notably, the Personal Information Protection Act does not treat data security violations as injuries to property, nor does it treat such violations in a manner similar to violations of biometric information regulations under the Biometric Privacy Act (where a violation of the act is actionable without requiring a plaintiff to demonstrate an injury). Instead, the Personal Information Protection Act treats violations as consumer injuries. The General Assembly has carved out special standing rules for other types of informational injuries but has not done so for the underlying data in this case.

¶ 62 Adopting plaintiffs’ diminution theory, based on the allegations before us, would create a rule that any data breach exposing similar PII/PHI would be *per se* actionable because plaintiffs allege that the data breach alone depresses the apparent market value of their data. That result is not consistent with Illinois case law or the regulatory scheme, and we cannot endorse it.

¶ 63 We are also skeptical of plaintiffs’ theory for other reasons described by our colleagues in the Fifth District: plaintiffs have not alleged that they could sell their personal information for value, and there is no nonspeculative way to assess the lost value. *Petta*, 2023 IL App (5th)

220742, ¶ 17. The injury is too abstract, speculative, and unsupported to constitute a concrete injury. *Id.*

¶ 64 5. Plaintiffs' Overpayment Theory Is Forfeited on Appeal

¶ 65 Plaintiffs pled that defendants' failure to protect their data prevented plaintiffs from getting the full benefit of their bargain with CCH. Plaintiffs claim they conferred a monetary benefit to CCH where they paid for services and part of the consideration for their payment was adequate data security for information collected by CCH. Because defendants failed to protect plaintiffs' data, plaintiffs assert that they overpaid CCH—that CCH received the full benefit of the bargain while plaintiffs did not.

¶ 66 On appeal, plaintiffs did not raise their overpayment theory or furnish any authority in support of it. As a result, the argument was forfeited, and we do not reach it. Ill. S. Ct. R. 341(h)(7) (eff. Oct. 1, 2020) (points not argued on appeal are forfeited); see *Cordeck Sales, Inc. v. Construction Systems, Inc.*, 382 Ill. App. 3d 334, 361 (2008).

¶ 67 III. CONCLUSION

¶ 68 Because we find that plaintiffs lack an injury-in-fact or an injury fairly traceable to defendant's conduct, we affirm the trial court's dismissal for lack of standing. Plaintiffs did not ask that the case be remanded with instructions to allow an amended complaint, so we do not remand for amendments to the pleadings.

¶ 69 Affirmed.

Kimber v. Cook County Health & Hospitals System, 2026 IL App (1st) 251091

Decision Under Review: Appeal from the Circuit Court of Cook County, No. 2023-CH-09293; the Hon. Caroline K. Moreland, Judge, presiding.

**Attorneys
for
Appellant:** Ben Barnow, Anthony L. Parkhill, Riley W. Prince, and Nicholas W. Blue, of Barnow and Associates, P.C., and William J. Edelman, of Milberg, PLLC, both of Chicago, for appellants.

**Attorneys
for
Appellee:** Scott L. Schmookler and Meagan P. VanderWeele, Special Assistant State's Attorneys, of Gordon Rees Scully Mansukhani, of Chicago, for appellee Cook County Health and Hospitals System.

Peter Drever, of Cozen O'Connor, of Chicago, for other appellee.
