Case No. 130337

In the Supreme Court of Illinois

REBECCA PETTA, on her own behalf and on behalf of those similarly situated,

Plaintiff-Appellant,

v.

CHRISTIE BUSINESS HOLDINGS COMPANY, P.C., d/b/a CHRISTIE CLINIC,

Defendant-Appellee.

On appeal from the Illinois Appellate Court, Fifth Judicial District, Case No. 5-22-0742, there on appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, Case No. 22-LA-51, Hon. Jason M. Bohm, Judge Presiding

APPELLEE'S BRIEF

Jonathan B. Amarilio
Jeffrey M. Schieber
Jaimin H. Shah
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker Drive, Suite 2600
Chicago, Illinois 60601
Tel.: 312.527.4000
jamarilio@taftlaw.com
jschieber@taftlaw.com
jshah@taftlaw.com
Attorneys for Defendant-Appellee

E-FILED
8/15/2024 12:06 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS &
POINTS AND AUTHORITIES

Page

NATURE OF THE CASE

This is a data breach case. Physician-owned medical practice group Christie Business Holdings Company, P.C., doing business as Christie Clinic ("Christie"), was the victim of a data breach about three years ago. C86-87. When Christie learned of the breach, it launched a thorough forensic investigation and notified all necessary governmental authorities as well as potentially affected individuals, offering them free credit monitoring and identity protection for their ease of mind. C114-19. Christie patient Rebecca Petta nonetheless sued Christie, claiming her sensitive personal information was compromised by the hackers and Christie was at fault. She asserted several causes action for negligence and violation of Illinois' data breach statute. C81-112. The circuit court dismissed plaintiff's complaint for failure to state a claim and the appellate court affirmed, holding plaintiff lacked standing to bring her claims. C432-44; A7-18. This Court granted her leave to appeal.

ISSUES PRESENTED

1. Whether plaintiff has adequately pleaded that her sensitive health and personally identifiable information was stolen during the attack on Christie and subsequently misused.

2. Whether plaintiff has standing to sue.

3. Whether plaintiff may bring common law negligence claims premised on the alleged failure to safeguard sensitive personal information.

4. Whether plaintiff has preserved for review the issue of whether her claim is barred by the economic loss doctrine and, if so, whether that doctrine bars her tort claims.

STATEMENT OF FACTS

Plaintiff's statement of facts takes many liberties, straying far from the allegations of her own complaint. These are the pertinent facts and plaintiff's actual allegations, well-pleaded and otherwise:

A. The data breach and Christie's response.

Christie is a physician-owned medical practice group providing care to patients in central Illinois. C86. Approximately three years ago, Christie was the victim of a data breach. C87. When Christie learned of the breach, it hired a leading data forensics firm, launched a thorough forensic investigation to determine the nature and scope of the attack, and notified federal and state governmental authorities as well as potentially affected patients. C82; C114.[1]

The investigation confirmed that the attack did not expose any patient's electronic medical records and the bad actor did not have access to Christie's patient portal or its computer network. C114-19. The investigation also confirmed that the purpose of the attack was not to obtain medical records or other sensitive health or personally identifiable information, but rather to intercept a business transaction between Christie and a third-party vendor. *Id*.

[1] Facts recounting the data breach are taken from the complaint and the "Notice of Data Incident" attached as an exhibit thereto. C83, n.3.

The criminal was, in other words, attempting to commit wire fraud, not steal patients' personal information. There was no evidence—none—of identity theft or misuse of patients' sensitive health and personally identifiable information as a result of the attack. *Id.*

In their attempt to intercept the payment from Christie to its vendor, the criminal had access to only one Christie employee email account. *Id.* Although Christie could not determine if the criminal viewed any emails containing patient information, Christie reviewed the full scope of information in the affected email account. *Id.* Christie determined that that the impacted email account "*MAY* have contained" some patients' personal information, including names, addresses, Social Security numbers, medical information, and health insurance information. *Id.* (emphasis original). Although there was no evidence of identity theft or misuse of personally identifiable information, or even intent to steal such information, Christie provided notice to all potentially affected persons and offered them free credit monitoring and identity protection services, including identity theft insurance, for their comfort and ease of mind. *Id.*

B. Plaintiff's lawsuit.

Plaintiff responded to the notice by suing Christie on behalf of herself and a putative class, bringing claims for: (1) common law negligence; (2) negligence *per se* for violation of the Federal Trade Commission Act (15 U.S.C. § 41 *et seq.*) ("FTC Act"); (3) negligence *per se* for violation of the Health

Insurance Portability and Accountability Act (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) ("HIPAA"); and (4) violation of the Illinois Personal Information Protection Act (815 ILCS 505/1 *et seq*.) ("PIPA"). C81-112. Plaintiff sought unspecified damages and injunctive relief requiring Christie to obey information privacy laws and further extend its offer to provide free identity theft protection and credit monitoring services. *Id*.

The allegations made in plaintiff's complaint are at times confusing because they are often self-contradictory and incompatible with her characterizations thereof in her appellant's brief. There are nonetheless two key allegations in plaintiff's complaint that merit close attention.

Plaintiff's first key allegation is that her sensitive health and personally identifiable information was exfiltrated (*i.e.*, stolen) by the bad actor who attacked Christie. Plaintiff alleges that Christie "confirmed" that the criminal "successfully stole" her and others' personal information, which was thereby "compromised" and "disclosed" to the criminal. C82-85 ¶¶ 2, 4, 10, 18. Plaintiff also alleges with less certainty that the information contained in the hacked employee's email account "may have contained" patients' personal information and the bad actor "likely" accessed and stole such information. C84 ¶ 9; C88 ¶ 29. She does not explain this discrepancy. Regardless, this first key allegation is based on her assertion—made upon information and belief—that "malicious actors maintained unfettered access to Christie Clinic's network and copied

and exported substantial amounts of" patients' sensitive health and personally identifiable information. C87-88 ¶ 28.

Plaintiff's second key allegation addresses her claimed harm and bears quotation:

> Since the Data Breach, Petta has experienced suspicious behavior in connection with her phone number and address. Her phone number, city, and state have been used in connection with a loan application at First Financial Bank, Columbus, Ohio, in someone else's name. Petta received multiple phone calls in recent months regarding loan applications she did not initiate.

C85 ¶ 18. Although plaintiff makes reference to the use of her "address" in this allegation, the follow-on sentence clarifies that she means only her city and state (*i.e.*, her hometown).

Plaintiff does not allege that any non-public or sensitive information was misused. For example, she does not allege that her Social Security number was used in any loan application. Plaintiff does not allege that her name was misused. She also does not allege when the loan applications or phone calls were made or when she learned of the applications. Plaintiff likewise does not allege the loan applications were approved—presumably not—or that they impacted her finances or credit. And she does not allege that any other "suspicious" activity occurred. Thus, according to plaintiff, phone calls she received at some unspecified time(s) about one or more loan applications made in someone else's name at some unspecified time(s), without using her Social Security number or other private or sensitive personal information, evidence that she is the victim of identity theft.

Plaintiff also variously alleges that she faces "both short-term and long-term risk of identify theft," which she describes as "ongoing," imminent," and "certainly impending." C89 ¶ 37; C104-05 ¶ 93; C109 ¶ 119. Plaintiff makes a host of general allegations discussing the dangers of identity theft in ostensible support of her fear of future harm, without connecting those evils to any specific factual allegations concerning her experience following the data breach at issue. C89-96 ¶¶ 39-62. And, without providing any relevant facts, she alleges that she has been harmed by: paying out-of-pocket expenses to mitigate her increased risk of identity theft and fraud; the lost value of her time spent mitigating that risk; "decreased credit scores and ratings"; and "irrecoverable financial losses due to fraud." C104-05 ¶ 93; C109 ¶ 119.

Plaintiff adds for the first time in her appellant's brief here that the bad actor used her name and mailing address, and "may have also used her social security number," in connection with the unsuccessful loan applications. Pl.'s Br. 1, 8, 12. Plaintiff says she pleaded this in her complaint. She did not. Plaintiff does not mention the misuse of her Social Security number or mailing address in her complaint, and she pleaded the loan applications were made "in someone else's name." C85 ¶ 18. Plaintiff nevertheless argues in her statement of facts that the (unpleaded) use of her name, mailing address, and Social Security number show "the hackers undoubtedly succeeded in obtaining her private information from Christie during the Data Breach." Pl.'s Br. 8.

C. Procedural history.

Plaintiff's complaint was consolidated with a similar complaint brought by a Jane Doe. C190. Christie moved to dismiss both actions for lack of standing and legal insufficiency pursuant to 735 ILCS 5/2-619.1. C262-90. In opposing these motions, plaintiff never requested leave to amend as an alternative to dismissal with prejudice. *See* C291-321. The circuit court dismissed Doe's complaint for lack of standing pursuant to *Maglio v. Advocate Health and Hospitals Corporation*, 2015 IL App (2d) 140782. The circuit court found plaintiff's complaint could survive initial standing scrutiny, but nevertheless failed to state a valid claim pursuant to *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358, 362 (1st Dist. 2010), which held that neither PIPA, HIPAA, the FTC Act, nor the common law permit the type of action brought here. C432-41; C443-44. The circuit court alternatively found the economic loss doctrine barred plaintiff's negligence claim. C442-43.

The circuit court commented that plaintiff did not request leave to amend, and although it might ordinarily grant leave, judicial economy weighed in favor of allowing the appellate court to review its conclusions. C444. Plaintiff never sought leave to amend attaching a proposed amended complaint curing the deficiencies addressed by the court, nor did she file a motion to reconsider requesting such relief. Plaintiff and Doe appealed. C445.

The appellate court affirmed. Plaintiff says in her statement of facts that the appellate court "reversed" the circuit court's dismissal of her complaint.

Pl.'s Br. 10. It did not. The appellate court affirmed the dismissal of her complaint on different grounds, namely, standing. A14-18. Plaintiff also says the appellate court's analysis turned on its "quick Google search" and traceability finding. Pl.'s Br. 10. This too is wrong. Drawing on its analysis of the shortcomings of the Doe's similar complaint, the appellate court held that plaintiff's allegations of the threat of future harm and damages fell short of the standing requirements applied in *Maglio* because they were speculative and conclusory, and her allegations concerning the loan applications were too threadbare to satisfy Illinois' fact-pleading standards. A14-18. The court observed that plaintiff's complaint is missing several essential factual allegations, including an allegation that any of plaintiff's sensitive personally identifiable information was misused in the unsuccessful loan applications, allegations connecting the unsuccessful loan applications to the Christie data breach, and allegations concerning her claim to damages. A15-16.

The appellate court alternatively added that it saw no way plaintiff could in good faith allege the unsuccessful loan applications are fairly traceable to Christie's alleged conduct given that the information plaintiff said was used in the loan applications (her phone number and hometown) is readily, publicly available, including by way of a "quick Google search." A15-16. The reviewing court said plaintiff's claims are thus "purely speculative" as "[t]here is no way, outside of speculating" to determine that the information used on the loan

applications was obtained from the attack on Christie. A16. "The information would still have been public had this breach not occurred." *Id.*

Plaintiff then filed a petition for leave to appeal, which was granted.

ARGUMENT

Plaintiff's petition for leave to appeal was premised on the argument that a conflict exists between the appellate court's First and Fifth judicial districts concerning the requirements for standing in data breach actions. This, in turn, was based on plaintiff's representations to this Court that she had properly alleged her sensitive personal information was stolen from Christie and later criminally misused. Plaintiff argued the Fifth District in this case held such circumstances are insufficient to confer standing, while the First District in *Flores v. Aon Corporation*, 2023 IL App (1st) 230140, reached the opposite conclusion. However, as discussed below, the factual underpinnings of plaintiff's argument for review are false. The case she described in her petition, and which she continues to describe in her appellant's brief, is not the case alleged in her complaint. Christie thus respectfully suggests that the Court may wish to entertain the possibility that review in this case was improvidently granted.

Should the Court decide that review was properly granted, it will still be confronted with several additional problems with plaintiff's claims. First among these is plaintiff's failure to properly allege that her sensitive personal information was actually stolen and misused. Further, plaintiff lacks standing

because she has not suffered an injury-in-fact, but rather complains only of a non-actionable and speculative risk of future injury. If that were not enough, she also impermissibly attempts to use negligence law as an end-run around the rights and remedies the Illinois General Assembly specifically created for data breach victims. And her tort claims are, in any event, barred by the economic loss doctrine. For all these reasons, the dismissal of plaintiff's complaint was more than justified and should be affirmed.

I. The case plaintiff presents to this Court is not the case alleged in her complaint, which is insufficiently pleaded.

This dispute presents several issues that may have attracted the Court's interest. However, it must be said at the outset that this case can, and probably should, be decided on comparatively unexceptional grounds—plaintiff's failure to properly plead her claims, making this case a poor opportunity for deciding any novel legal issues. As the adage goes, "bad facts often make bad law." *People v. DiCorpo*, 2020 IL App (1st) 172082, ¶ 48.

Plaintiff tells the Court throughout her appellant's brief that the criminal who attacked Christie successfully stole her sensitive health and personally identifiable information, and that same information (including her name, mailing address, and possibly her Social Security number) was then used in one or more loan applications she did not initiate. *See*, *e.g.*, Pl.'s Br. 1, 8, 10, 12, 14, 22. Plaintiff's issues statement and arguments are all constructed around this central framework, and she severely criticizes the appellate court

for supposedly ignoring these facts and failing to draw reasonable inferences therefrom in her favor. *See*, *e.g.*, Pl.'s Br. 2, 17-20.

But before the Court can reach the issues plaintiff asks it to resolve, the Court must grapple with the fact that plaintiff has *never* properly alleged that her sensitive personal information was actually stolen from Christie, much less that it was misused in acts of identity theft or fraud. This means that none of the questions plaintiff raises in her brief are properly before the Court and all of her arguments are, at best, immaterial.

A. Plaintiff has not properly pleaded that her sensitive personal information was stolen from Christie.

This is a data breach case, making an allegation that plaintiff's sensitive health and personally identifiable information was actually stolen from Christie the indispensable factual predicate of all her claims. And yet plaintiff has failed to sufficiently plead that fact. Without that, plaintiff cannot plausibly allege breach, causation, damages, or any of the most basic elements of common law negligence, negligence *per se*, and violation of PIPA. Put simply, without a properly-pleaded allegation on this point, plaintiff has no claims.

"Illinois is a fact-pleading jurisdiction." *Simpkins v. CSX Transp., Inc.*, 2012 IL 110662, ¶ 26. "While this does not require the plaintiff to set forth evidence in the complaint, it does demand that the plaintiff allege facts sufficient to bring a claim within a legally recognized cause of action." *Id.* "A plaintiff may not rely on conclusions of law or fact unsupported by specific factual allegations." *Id.* Only "well-pled facts" and "reasonable inferences that

may be drawn from those facts" are taken as true. *Id.* ¶ 26; *accord In re Estate of Powell*, 2014 IL 115997, ¶ 12 ("a court cannot accept as true mere conclusions unsupported by specific facts").

The Court need not look beyond the four corners of the complaint to see that plaintiff's conclusion that her sensitive personal information was stolen from Christie is based on one, central allegation. Specifically, plaintiff pleads on "information and belief" that "malicious actors maintained unfettered access to Christie Clinic's network and copied and exported substantial amounts of" patients' sensitive health and personally identifiable information during the attack. C87-88 ¶ 28. This is an issue of ultimate fact. If plaintiff cannot eventually prove it, she cannot recover. *See Givens v. City of Chicago*, 2023 IL 127837, ¶ 70 (an ultimate fact is one that controls a general verdict). And, by the same token, if plaintiff cannot properly plead this ultimate fact, she cannot proceed. *People ex rel. Scott v. College Hills Corp.*, 91 Ill. 2d 138, 145 (1982).

"An allegation made on information and belief is not equivalent to an allegation of relevant fact." *Patrick Eng'g, Inc. v. City of Naperville*, 2012 IL 113148, ¶ 40 (cleaned up). Plaintiffs at the pleadings stage may not have the benefit of discovery tools to expose facts only known to a defendant, but "[a] plaintiff will have knowledge of what it did to learn those details" and those efforts must be pleaded to successfully state a claim. *Id.*; *accord In re Estate of DiMatteo*, 2013 IL App (1st) 122948, ¶ 83. Without such allegations, a court

cannot "determine whether [an] allegation is anything more than mere speculation," and it cannot survive a motion to dismiss. *In re Marriage of Reicher*, 2021 IL App (2d) 200454, ¶¶ 42-43.

Plaintiff here does not plead, as she must, any facts concerning what efforts she took to discover whether her information was actually stolen during the attack on Christie. Her naked assertion made on information and belief, devoid of factual substance, is all she offers. As a matter of law, this is not enough. While she repeats many times throughout her complaint that her information was stolen, all those assertions trace back to this singular, insufficiently-pleaded allegation.

Plaintiff attempts to paper-over this insufficiency by arguing she will know more after discovery and by pointing to the Notice of Data Breach Incident, which she attaches as an exhibit to her complaint and incorporates by repeatedly referencing its contents. *See*, *e.g.*, C82, n*1; C83, n*2-6; C87, n.15-19; Pl.'s Br. 19, n.4. She similarly cites to electronic versions of the same notice posted on the internet. But the notice self-evidently refutes, rather than supports, plaintiff's allegation that her sensitive personal information was stolen. It says that Christie's investigation confirmed the bad actor *did not* have access to Christie's computer network or patient portal and the attack *did not* expose any patient's electronic medical records. C114. The purpose of the attack was *not* to obtain medical records or other sensitive patient information, but rather to intercept a business transaction between Christie

and a vendor. *Id*. And although Christie could not determine if the criminal incidentally *viewed* any emails in that account *potentially* containing sensitive patient information, there was *no evidence* of identity theft or misuse of patients' personal information as a result of the attack. *Id*.

Documents and exhibits attached to pleadings are part of the pleadings. *Bajwa v. Metropolitan Life Ins. Co*., 208 Ill. 2d 414, 432 (2004) (cleaned up). Even when, as here, a claim is not founded upon the attached document, the document is still treated as part of the pleading if incorporated therein. *Id*. It is an "integral part of the complaint and must be so considered." *Fowley v. Braden*, 4 Ill. 2d 355, 360 (1954). If the complaint and exhibit are inconsistent, neither controls, and the allegations are deficient. *Id*.

Plaintiff's allegations about the Notice of Data Breach Incident are diametrically opposed to its actual contents. Any attempt she makes, based on the notice, to argue that she has alleged her sensitive personal information was stolen from Christie's network are thus a nullity, if not deliberately misleading. To be clear, the point here is not that the notice affirmatively defeats plaintiff's allegations, but rather that the notice does nothing to save plaintiff's insufficiently-pleaded allegation, made on information and belief, that her information was stolen.

Because plaintiff's key conclusion that her sensitive health and personally identifiable information was stolen is insufficiently pleaded, her complaint is missing its factual nexus, making it exactly the kind of "fishing

expedition" Illinois courts rightly disallow. *In re Marriage of Reicher*, 2021 IL App (2d) 200454, ¶ 43. After all, if plaintiff's sensitive information was not stolen from Christie, then anything allegedly done using that information cannot be Christie's fault. "There is," to borrow a phrase, "no there there." Gertrude Stein, *Everybody's Autobiography* 289, Cooper Sq. Pub. Inc. 1971. The Court need go no further than this to affirm the dismissal of the complaint.

Plaintiff will argue otherwise, either doubling down on her misrepresentations of her own complaint or attempting to couch what amounts to a notice pleading standard as supposedly reasonable inferences. But the complaint speaks for itself, and it says nothing helpful to her. Plaintiff may also argue that she should now be given leave to amend to correct these failings, if she can. However, it bears reminding that plaintiff *never* sought that relief from the trial court, the appellate court, or this Court, much less offered to demonstrate how she might cure her pleading deficiencies. She instead persists in mischaracterizing her own complaint even now. By any measure, plaintiff has forfeited her right to request leave to amend for the first time in her supreme court reply brief. Ill. S. Ct. R. 341(h)(7) ("[p]oints not argued are forfeited and shall not be raised in a reply brief, in oral argument, or on petition for rehearing"); *see also NAV Consulting, Inc. v. Sudrania Fund Svcs. Corp.*, 2023 IL App (1st) 211015-U, ¶ 55 (affirming dismissal with prejudice where plaintiff failed to attach proposed amended complaint to motion to amend).

B. Plaintiff also fails to allege that her sensitive personal information was misused.

Plaintiff also cannot overcome the fact that she fails to plead that her sensitive personal information was ever misused. This points bears emphasis. Plaintiff has *never* actually alleged anything that could be reasonably described as identity theft or fraud. This failure colors every issue before the Court because, when the allegations of plaintiff's complaint are compared to the questions she asks this Court to answer, it is apparent that she is essentially seeking an advisory opinion.

There are two types of personally identifiable information: sensitive and non-sensitive. These are exactly what one would expect them to be. Sensitive information is *non-public* information that can be used to harm an individual (*e.g.*, Social Security numbers, driver's license numbers, passport numbers, biometric data, and financial information), while non-sensitive information is publicly-available information permitting the identity of an individual to be directly or indirectly inferred (*e.g.*, names, telephone numbers, email addresses). United States Dep't of Homeland Security, Privacy Office, *DHS Handbook for Safeguarding Sensitive PII*, at 5 (Dec. 4, 2017), *available at* https://tinyurl.com/4k8f9r45; *Kim v. McDonald's USA, LLC*, Case No. 21-cv-05287, 2022 WL 4482826, at *5 (N.D. Ill. Sept. 27, 2022).

The Illinois Personal Information Protection Act ("PIPA"), which governs the handling of personally identifiable information, uses the term "personal information" in lieu of the more cumbersome "sensitive personally

identifiable information" to mean names used in combination with: Social Security numbers; drivers license numbers; state identification numbers; banking account numbers combined with security codes or access passwords; medical information; health insurance information; and unique biometric information. 815 ILCS 530/5. The statute is clear that personal information "does *not* include publicly available information" lawfully made available. *Id.* (emphasis added).

Identity theft occurs when a person uses another's sensitive personal information without permission to steal the victim's identity. This stolen identity is then used to commit credit fraud, fraudulently withdraw funds from bank accounts, steal tax refunds, and wrongfully obtain other funds, goods, and services. *See* USAGov, *Identity Theft* (May 3, 2024), *available at* https://tinyurl.com/uzhv7stb (defining identity theft); Federal Trade Commission, Consumer Advice, *What to Know About Identity Theft* (April 2021), *available at* https://tinyurl.com/brx8t8y2 (same); U.S. Dep't of Justice, Criminal Division, Fraud Section, *Identity Theft* (Aug. 11, 2023), *available at* https://tinyurl.com/ycypsnbw (same).

Here, plaintiff has not alleged that *her* sensitive health or personally identifiable information was used in the loan application she alleges was made in someone else's name. She alleges only that her phone number and hometown were listed in one such application and that she "received multiple phone calls … regarding loan applications she did not initiate." C85 ¶ 18. Contrary to the

many misstatements in her brief, plaintiff does not allege that any of her sensitive personal information, such as her Social Security number, was misused in any loan application. She does not even allege that her name was used—she alleges the application was made "in someone else's name." *Id.* As its label unmistakably implies, identity theft occurs when someone attempts to pass themselves off as their victim. Whatever it is that plaintiff believes occurred here, it is not identity theft.

The ramifications of this failure on plaintiff's appeal are decisive. It goes without saying that plaintiff cannot represent a class of persons who have allegedly had their sensitive personal information misused unless her sensitive personal information was also misused. *Griffith v. Wilmette Harbor Ass'n, Inc.*, 378 Ill. App. 3d 173, 184 (1st Dist. 2007). More importantly, plaintiff asks this Court to decide several legal questions premised on the assumption that her sensitive personal information was actually misused. Pl.'s Br. 2. Every argument she now presents is based on this notion. But when plaintiff's complaint is read, no allegation to that effect is found and none can be reasonably inferred. All the contrary representations made in plaintiff's brief are demonstrably false.

There is a term for the type of decision plaintiff seeks from this Court: an advisory opinion. *See People ex rel. Partee v. Murphy*, 133 Ill. 2d 402, 408 (1990) ("[a]n advisory opinion results if the court resolves a question of law which is not presented by the facts of the case"). This Court does not issue

advisory opinions. *Id.*; *Commonwealth Ed. Co. v. Ill. Commerce Comm'n*, 2016 IL 118129, ¶ 10 (same); *see also Murthy v. Missouri*, 144 S.Ct. 1972, 1985 (2024) ("if a dispute is not a proper case or controversy, the courts have no business deciding it, or expounding the law in the course of doing so") (cleaned up). And for the reasons discussed above, it is far too late for plaintiff to seek leave to amend. *Supra* 15. Christie therefore respectfully suggests that for this reason as well, this case presents a poor opportunity for deciding the larger legal issues that may have interested the Court when granting leave to appeal, and the appeal should consequently be dismissed as improvidently granted.

II. Plaintiff does not have standing to sue.

Plaintiff has no standing to sue. The standing doctrine is an indispensable component of justiciability. *Lebron v. Gottlieb Mem. Hosp.*, 237 Ill. 2d 217, 265 (2010) (Karmeier, J., concurring in part). A "justiciable matter is a controversy appropriate for review by the court, in that it is definite and concrete, as opposed to hypothetical or moot, touching upon the legal relations of parties having adverse legal interests." *Id.* at 264 (cleaned up). To be sufficiently definite and concrete to make a matter justiciable, standing requires "some injury in fact to a legally cognizable interest." *Greer v. Ill. Housing Dev't Auth.*, 122 Ill. 2d 462, 492 (1988); *see also Rowe v. Raoul*, 2023 IL 129248, ¶ 61 ("Stated more simply: No injury caused by defendant, no standing for plaintiff.") (O'Brien, J., concurring).

Because plaintiff has not actually alleged that her supposedly stolen sensitive health or personally identifiable information was misused, *all* of the arguments she attempts to advance in her brief based on the notion that her sensitive information was the subject of misuse are irrelevant. *See* Pl.'s Br. 11-27. That fact pattern does not map to this complaint. *See Allen v. Wright*, 468 U.S. 737, 752 (1984) (standing analysis requiring careful examination of a complaint's allegations), *overruled in part on other grounds*. Those arguments are not properly before the Court. We are thus left with, at most, only plaintiff's allegations that her publicly-available, non-sensitive personal information was misused, and she is at an increased risk of future identity theft or fraud as an asserted basis potentially conferring standing. Pl.'s Br. 25.[2] But this falls short of the mark. Standing is made of sterner stuff.

A. Plaintiff lacks standing because she has not suffered an injury-in-fact.

Plaintiff has not suffered an injury-in-fact to a legally cognizable interest. "An injury-in-fact is an actual or imminent invasion of a legally protected interest, in contrast to an invasion that is conjectural or

---

[2] Should plaintiff argue she was harmed by receiving the "multiple phone calls" referenced in her complaint (C85 ¶ 18), courts have generally rejected such *de minimis* claims. *See*, *e.g.*, *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022) ("Courts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact."); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (same); *Jackson v. Loews Hotels, Inc.*, No. ED-CV-827-DMG (JCx), 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (same); *c.f. Flores*, 2023 IL App (1st) 230140, ¶ 42 (finding such claims are not actual damages). Unsolicited phone calls are an annoying part of modern life, but they are not an injury-in-fact.

hypothetical." *Injury-in-fact*, Black's Law Dictionary 856 (9th ed. 2009). The claimed injury, whether actual or threatened must be: (1) "distinct and palpable"; (2) "fairly traceable" to the defendant's actions; and (3) "substantially likely to be prevented or redressed by the grant of the requested relief." *Greer*, 122 Ill. 2d at 492-93 (cleaned up). Justice Sandra Day O'Connor once explained that standing analysis asks: "Is the injury too abstract, or otherwise not appropriate, to be considered judicially cognizable? Is the line of causation between the illegal conduct and injury too attenuated? Is the prospect of obtaining relief from the injury as a result of a favorable ruling too speculative?" *Allen*, 468 U.S. at 752.

These inquiries all get at the same point. The standing doctrine exists in the first instance to ensure that claims cannot be pursued unless some very real injury-in-fact has been suffered or imminently will be suffered. This means that speculative "some day" injuries—such as increased risk of future identity theft following a data breach—are not themselves injuries and are thus insufficient to confer standing. *See Berry v. City of Chicago*, 2020 IL 124999, ¶¶ 32-33 (an increased risk of future harm is not an injury). If an injury has not occurred and is only threatened, the plaintiff must be "in *immediate* danger of sustaining a direct injury" to have standing to sue. *Chicago Teachers Union, Local 1 v. Bd. of Edu. of City of Chicago*, 189 Ill. 2d 200, 206 (2000) (emphasis added). Plaintiff's case does not pass this test and she cannot reasonably plead otherwise.

1. Increased risk of future identity theft or fraud is not a distinct and palpable injury.

Illinois law on standing in the data breach context is sparse, but one note rings clearly throughout: no concrete harm, no standing. The leading case is *Maglio v. Advocate Health and Hospitals Corporation*, 2015 IL App (2d) 140782, *pet. for leave to app. den'd*. That case was brought after burglars broke into a hospital administrative building and stole computers containing the personal information of four million patients, several of whom sued asserting claims similar to those brought here, including negligence and violation of PIPA. *Id.* ¶¶ 1-3. As here, the plaintiffs alleged that the hospital system had negligent data security practices and thereby facilitated the disclosure of sensitive patient information. *Id.* ¶ 5. As here, the plaintiffs alleged they faced an increased risk of identity theft and fraud, and lost time and money mitigating that risk. *Id.* ¶¶ 10, 12. As here, the plaintiffs did not allege any misuse of their sensitive personal information; that is, they did not allege that they had yet been victims of actual or attempted identity theft or fraud. *Id.* ¶ 5. This alone distinguishes *Maglio* and the instant case from *Flores*, upon which plaintiff so heavily relies, and which involved plaintiffs who had already experienced actual identity theft and fraud. *Flores*, 2023 IL App (1st) 230140, ¶ 15.

The circuit court in *Maglio* dismissed the plaintiffs' claims for lack of standing and the appellate court affirmed. Relying on this Court's precedent in *Greer* and *Chicago Teachers Union*, *supra*, the reviewing court found the

plaintiffs suffered no injury-in-fact sufficiently distinct and palpable to confer standing. *Maglio*, 2015 IL App (2d) 140782, ¶¶ 22-23. The plaintiffs' claimed injury—an increased risk of identity theft or fraud—was by its very nature unrealized, and the plaintiffs could not adequately plead it was certainly impending or imminent, making it "purely speculative and conclusory, as no such identity theft has occurred to any of the plaintiffs." *Maglio*, 2015 IL App (2d) 140782, ¶¶ 23-25. If this sounds familiar, it is because *Maglio* is directly on point.

The *Maglio* court also found instructive federal standing jurisprudence, which occasionally differs from Illinois' standards, but not here. In a line of decisions solidified over the last decade, the United States Supreme Court has explained that an injury is sufficient for standing if it is "concrete and particularized" and "actual and imminent, not conjectural or hypothetical." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (cleaned up). When considering whether a threatened injury is "imminent," that concept "cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (cleaned up). This means that "[a]n allegation of future injury may suffice if the threatened injury is certainly impending or there is a substantial risk that harm will occur." *Susan B. Anthony*, 573 U.S. at 158 (cleaned up). But "[a]llegations of possible future injury are not sufficient." ." *Clapper v*, 568 U.S. at 409 (cleaned up); *see also TransUnion v. Ramirez*, 594 U.S. 413, 436-37

(2021) (risk of future harm is insufficient to establish standing for damages claims).

Agreeing with the Supreme Court, the appellate court in *Maglio* explained that even when it is objectively reasonable to expect a future injury could occur, finding standing based on nothing more than that expectation is fundamentally "inconsistent with the requirement that the threatened injury be certainly impending to constitute an injury-in-fact." 2015 IL App (2d) 140782, ¶ 25. Any theory that "relies on a highly attenuated chain of events" fails as a matter of law. *Id.* (citing *Clapper*, 586 U.S. at 408-10, and *Peters v. St. Joseph Services Corp.*, 74 F. Supp. 3d 847, 856-57 (S.D. Tex. 2015) (putative class action against hospital system following data breach dismissed for lack of standing because the heightened risk of future identity theft/fraud posed by the data breach did not confer standing on persons whose information merely might have been accessed)).

The *Maglio* court thus explained that "[a]n increased risk or credible threat of impending harm is plainly different from certainly impending harm, and *certainly impending* harm" is what standing requires. 2015 IL App (2d) 140782, ¶ 26 (cleaned up) (emphasis added); *accord Flores*, 2023 IL App (1st) 230140, ¶ 15 (fear of future identity theft or fraud, as opposed to actual misuse, is insufficient to confer standing); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42-46 (3d Cir. 2011) (same).

Here, the appellate court followed *Maglio* when holding that plaintiff lacks standing. It was right to do so. After finding plaintiff's allegations too conclusory and vague to satisfy Illinois' fact-pleading standard, the reviewing court found plaintiff's claims also failed for the same reasons as those of her (now former) co-plaintiff Doe. A14-15. In other words, plaintiff's claimed injury is "simply too speculative and not imminent" to confer standing because its adds up to nothing more than a risk of future harm. *Maglio*, 2015 IL App (2d) 140782, ¶ 15. Plaintiff's own complaint bears this out. She alleges that "[a]ccording to experts, one out of four data breach notification recipients becomes a victim of identity fraud." C89 ¶ 39. If there is a one-in-four chance of harm, then there is a three-in-four chance of no harm, meaning it is considerably more likely that harm will *not* occur. This cannot be reasonably characterized as "*certainly* impending" harm.

This is not meant to downplay the risks posed by identity theft, but merely to demonstrate that the risks are not themselves actionable. There is no question that millions of individuals are victimized by identity theft and fraud every year. However, the risk that plaintiff may some day be one of those victims does not constitute an *immediate* danger, much less one that is *certainly* impending, because that risk is contingent on a speculative chain of hypothetical events that may or may not materialize. Assuming, for the sake of argument, that her sensitive personal information was actually stolen from Christie, that chain of speculation includes assumptions that:

- plaintiff's sensitive personal information will be culled from the massive amount of patient information she says was stolen;
- her relevant information will then be sold by, or otherwise directly used by, the bad actor who attacked Christie;
- one of those bad actors will then select her personal information for misuse, and then actually misuse it; and
- that misuse will result in actual harm to plaintiff.

This is not an injury-in-fact. It is a hypothetical. It is speculation. Time will tell whether the risk plaintiff fears will eventually materialize into a concrete harm. If it does, then it might be said that an injury has been suffered and a cause accrued. But it is the harm itself, and not the mere risk of harm, that constitutes an injury—and that harm has not occurred here.

2. Increased risk of future harm is not an actual injury.

This Court's decision in *Berry v. City of Chicago*, 2020 IL 124999, controls. The plaintiffs in that case brought a class action against the city on behalf of a putative class comprised of all those living in an area where the city replaced lead water mains or meters. *Id.* ¶ 1. The plaintiffs claimed that the city was negligent in replacing that infrastructure and its negligence created an increased risk that lead would be dislodged or leach from service lines, subjecting the class to an increased risk of lead exposure. *Id.* ¶ 28. The city successfully moved to dismiss the complaint, the appellate court reversed, and this Court granted review.

The Court held that "an increased risk of harm is not, itself, an injury." *Id.* ¶ 33. Drawing on a well-established line of authority, it explained that "'an

increased risk of future harm is an *element of damages* that can be recovered for a present injury' but … such future risk 'is *not* the injury itself.'" *Id.* ¶ 32 (emphasis original) (quoting *Williams v. Manchester*, 228 Ill. 2d 404, 425 (2008)); *see also Lewis v. Lead Industries Ass'n*, 2020 IL 124107, ¶ 29 (unless and "[u]ntil the defendant's wrongful or negligent act produces injury … by way of loss or damage, no cause of action accrues"); *Bd. of Edu. of City of Chicago v. A, C & S, Inc.*, 131 Ill. 2d 428, 443 (1989) ("[t]he dangerousness which creates a risk of harm is insufficient standing alone to award damages"); *Boyd v. Travelers Insurance Co.*, 166 Ill. 2d 188, 197 (1995) ("[a] threat of future harm, not yet realized, is not actionable").

This is because "[t]he long-standing and primary purpose of tort law is not to punish or deter the creation of this risk but rather to compensate victims when the creation of risk tortiously manifests into harm." *Berry*, 2020 IL 124999, ¶ 33 (citing Oliver Wendell Holmes Jr., *The Common Law* 144 (1881)). "A person may pursue a cause of action in tort once harm occurs. Given this fact, there is little justification for imposing civil liability on one who only creates a risk of harm to others." *Id.* Further, "there are practical reasons for requiring a showing of actual or realized harm before permitting recovery in tort," including maintaining "a workable standard for judges and juries who must determine liability," "protect[ing] court dockets from becoming clogged with comparatively unimportant or trivial claims," and "reduc[ing] the threat of unlimited and unpredictable liability." *Id.* ¶ 34.

The same holds true here. For the reasons discussed above, plaintiff has never pleaded an actual injury. She alleges only an increased risk of possible future injury. And while plaintiff says that harm is "imminent" and "immediate," she alleges no facts supporting the use of those adjectives. *See* C84 ¶ 10; C104 ¶ 93; C109 ¶ 119. Including general allegations of the workings and evils of identity theft does not paper-over this failure because it does nothing to clarify the harm to plaintiff or its imminence *in this case*. *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 990 (W.D. Okla. 2021); *C.C. v. Med-Data Inc.*, No. 21-2301-DDC-GEB, 2022 WL 970862, at *7 (D. Kans., Mar. 31, 2022).

If plaintiff has her way, every person whose sensitive personal information is merely exposed in a data breach, or even potentially exposed, regardless of the nature of the data breach, will have a right of action in Illinois against their fellow victim—the institution attacked by bad actors. Plaintiffs will not need to allege or prove facts concerning the purpose or results of the breach. They will not need to allege or prove actual harm resulted from a breach. They will only need to allege and prove general allegations that the breach increased the risk that one day, if a certain hypothetical chain of events falls into place, they may be the victim of identity theft or fraud. That is not a workable standard, it does nothing to protect our courts from being clogged with an endless number of claims given the prevalence of data breaches, and

following large breaches it will result in unpredictable and unlimited liability. That cannot be the law.

Numerous sister states have come to the same conclusion, holding an increased risk of future harm without allegations or evidence of actual misuse insufficient to confer standing in data breach cases. *See*, *e.g.*, *Bradix v. Advanced Stores Co., Inc.*, 226 So.3d 523, 528-29 (La. App. 4th Cir. 2017); *Young v. Wetzel*, 260 A.3d 281, 287-88 (Penn. Commw. Ct. 2021); *Chatbot v. Spectrum Healthcare Partners, P.A.*, No. BCDWB-CV-2020-18, 2021 WL 659565, at *5 (Me. Jan. 14, 2021); *Abernathy v. Brandywine Urology Consultants, P.A.*, No. N20C-05-057 MMJ CCLD, 2021 WL 211144, at *4 (Del. Super. Ct. Jan. 21, 2021); *Rakyta v. Munson Healthcare*, No. 354831, 2021 WL 4808339, at *3-4 (Mich. Ct. App., Oct. 14, 2021); *Greco v. Syracuse ASC, LLC*, 218 A.D.3d 1156, 1157-58 (NY App. Div. 2023). Christie respectfully suggests this Court should do the same.

Given the nature of plaintiff's complaint, unless the Court is prepared to hold that the mere occurrence of a data breach is sufficient to constitute an injury-in-fact, it must affirm the result below. Doing so is the only way to preserve the most basic notions that have always animated Illinois' approach to standing.

3. Federal standing jurisprudence is instructive on this point.

i. The U.S. Supreme Court agrees that the risk of future harm does not confer standing.

Federal courts' approach to standing in data breach cases is evolving, but further along than Illinois law, and thus has some instructive value. The Supreme Court's decisions in *Clapper* and *TransUnion*, while not themselves data breach cases, are central to federal jurisprudence in this area.

Clapper involved a constitutional challenge to the Foreign Intelligence Surveillance Act brought by plaintiffs whose work required them to engage in sensitive communications potentially subject to federal surveillance. As discussed above, the decision turned on standing, which the Court held requires imminence, meaning a "threatened injury must be *certainly impending* to constitute injury in fact," making "allegations of *possible* future injury" insufficient. 568 U.S. at 409 (emphasis original) (cleaned up). Under this standard, even an "objectively reasonable likelihood" that a future injury will occur is inadequate. *Id.* at 410. A plaintiff cannot establish an imminent future injury for standing purposes when they "rel[y] on a highly attenuated chain of possibilities" or "speculation about the decisions of independent actors," even if that speculation is reasonable. *Id*. at 410-14; *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564 (1992) (claiming something will happen "some day" "is simply not enough" for standing).

Notably, *Clapper* also held that measures plaintiffs may take to protect themselves from possible, future injuries do not confer a present injury-in-fact. 568 U.S. at 415-416. Were the law otherwise, plaintiffs would be able to unilaterally lower the bar for standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 416. The Court was explicit that plaintiffs are not allowed to "manufacture standing" this way. *Id.*

The plaintiffs in *TransUnion* sued under the Fair Credit Report Act alleging the credit reporting agency maintained inaccurate reports indicating they were potential terrorists or serious criminals. There were two subsets of these plaintiffs. The first subset alleged TransUnion provided inaccurate reports to third-party businesses, resulting in actual harm akin to defamation. 594 U.S. at 417. The second subset alleged only that TransUnion maintained their inaccurate credit reports in its internal system, but had not yet provided those reports to any third parties. *Id.* at 418. The Supreme Court held that the second subset of plaintiffs did not have standing to pursue damages because they had suffered no concrete harm. *Id.* at 434. In so doing, the Court rejected the argument that the risk of future disclosure of the inaccurate reports constituted an injury, explaining again that "the mere risk of future harm, standing alone, cannot qualify as a concrete harm." *Id.* The plaintiffs in the second subset had not suffered a concrete harm that "materialized," and they

were not harmed merely by their exposure to the risk itself. *Id*. at 437. For the reasons discussed above, the same reasoning applies here. *Supra* 26-30.

It should be said that the Supreme Court distinguishes between claims seeking damages and those seeking injunctive relief when considering a party's standing. For injunctive claims, "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435. Whereas for damages claims, "the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm." *Id*. at 436. Illinois law arguably recognizes this same distinction, but forgives "lack of immediacy" when a plaintiff seeks declaratory and injunctive relief, although only for injuries that are distinct and palpable, including economic injuries. *Greer*, 122 Ill. 2d at 493-94. As discussed above, this does nothing to help plaintiff here because her claimed harm is not distinct and palpable (*supra* 22-30) and, as discussed below, she has no actual economic injuries (*infra* 51-52).

Regardless, plaintiff's request for injunctive relief is window dressing for her damages claims as she alleges nothing that would even arguably suggest that injunctive relief is appropriate. *Compare* C110 ¶ 123, *with Vaughn v. City of Carbondale*, 2016 IL 119181, ¶ 44 (reciting elements required for injunctive relief). For instance, she gives no clear basis for claiming the lack of adequate

legal remedy; one might reasonably ask why such a request does not contradict her demand for damages, and why, given her (inadequate) allegations that her sensitive personal information is now available to all on the dark web, another data breach would further harm her. Plaintiff merely requests that Christie be ordered to obey data privacy laws and regulations and offer more free identity theft and credit monitoring services. C109-11. This is, at most, an empty afterthought that does nothing to rescue plaintiff's standing. *See Greer*, 122 Ill. 2d at 492-93 (to have standing, a claimed injury must be "substantially likely to be prevented or redressed by the grant of the requested relief"); *Pardilla v. Village of Hoffman Estates*, 2023 IL App (1st) 211580, ¶ 35 (broad injunctions ordering a party to "obey the law" are invalid).

ii. Federal circuit court jurisprudence also cuts against plaintiff's standing.

Plaintiff argues that the decisions of several federal circuit courts support her standing here. She relies on these cases for the proposition that federal courts have found that victims of actual or attempted identity theft or fraud have standing to sue. Pl.'s Br. 15-16 (citing cases). However, as discussed above, that is not the case alleged in plaintiff's complaint. This authority thus does nothing to advance her cause.

The question presented here is whether an increased risk of future identity theft constitutes an injury-in-fact sufficient to confer standing. Without engaging in a circuit-by-circuit discussion on the subject, it is sufficient to note that multiple federal courts have already performed helpful

national surveys on this issue and arrived at different, but not necessarily inconsistent conclusions. Several courts have described the federal circuits as fairly evenly divided, with some having said at the pleadings stage that "a plaintiff can establish injury-in-fact based on the increased risk of identity theft" and others "declining to find standing on that theory." *Tsao*, 986 F.3d at 1340 (citing cases). Still others have noted that "although the circuits have diverged in result, the bases behind the differing decisions have several commonalities. That is to say, the differing sets of facts involved in each circuit's decision are what appear to have driven the ultimate decision on standing, not necessarily a fundamental disagreement on the law." *In re 21st Century Oncology Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1251 (M.D. Fl. 2019); *accord In re SuperValu, Inc.*, 870 F.3d 763, 769-71 (8th Cir. 2017) (agreeing and additionally finding United States Government Accountability Office report explaining that most data breaches do not result in identity theft did not support standing).

Whether this constitutes an actual split among the circuits matters less than the fact that even those courts that see a potential divide have recognized that the "cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data." *Tsao*, 986 F.3d at 1340. "[W]here no allegations of misuse are present, [federal] circuit courts have generally declined to find standing." *Legg*, 574 F. Supp. 3d at 990; *accord C.C. v. Med-Data*, 2022 WL

970862, at *4 (same); *Deevers Stoichev v. Wing Fin. Svcs., LLC*, No. 22-CV-0550-CVE-JFJ, 2023 WL 6133181, at *6 (N.D. Okla. Sept. 19, 2023) ("the majority of courts … have concluded that plaintiffs must allege actual misuse [] to demonstrate they face an imminent risk of fraud"); Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits*, 92 Notre Dame L. Rev. 1323, 1324 (2017) (same).

It should be said that the Seventh Circuit once agreed with plaintiff's alternative position here, holding in a case concerning a hack executed to obtain credit card information that "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an objectively reasonable likelihood that such an injury will occur." *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (cleaned up). However, that court has since walked back such analysis in light of the subsequent Supreme Court authority discussed above, which "makes clear that a risk of future harm, without more, is insufficiently concrete to permit standing to sue." *Ewing v. MED-1 Solutions, LCC*, 24 F.4th 1146, 1152 (7th Cir. 2022).[3] Several courts, including the appellate court in *Maglio*, accurately predicted this outcome. *See Maglio*, 2015 IL App (2d)

[3] *Remijas* and its progeny, *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), and *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829 (7th Cir. 2018), are also distinguishable because they involved circumstances in which actual instances of related fraud had already occurred following a data breach.

140782, ¶ 26; *Alonso v. Blue Sky Resorts, LLC,* 179 F. Supp. 3d 857, 864 (S.D. Ind. 2016).

What is clear is that any federal cases predating *TransUnion* that held the risk of future harm sufficient to confer standing in data breach cases for damages are no longer good law, regardless of whether the federal courts in question have since had the opportunity to say so explicitly. *See Vijender v. Wolf*, No. 19-cv-3337, 2020 WL 1935556, at *3 (D.D.C. Apr. 22, 2020) (recognizing that precedent may be "effectively overruled" when a later Supreme Court decision "eviscerates its reasoning") (cleaned up); *In re USAA Data Security Litig.*, 621 F. Supp. 3d 454, n.2 (S.D.N.Y. 2022) (recognizing that *TransUnion* abrogated the Second Circuit's decision in *McMorris v. Carlos Lopez & Assoc. LLC*, 995 F.3d 295 (2d Cir. 2021), which held an increased risk of identity theft or fraud constitutes an injury-in-fact). Standing cannot rest on overly broad assertions and breezy assumptions.

B. Plaintiff also lacks standing because there is no reasonable possibility of tracing her claimed injury to the Christie data breach.

To have standing to sue, a plaintiff must also be able to demonstrate that her claimed injury is "fairly traceable" to the defendant's alleged wrongdoing. *Greer*, 122 Ill. 2d at 492-93. "The whole purpose of the traceability requirement is to ensure that in fact, the asserted injury was the consequence of the defendants' actions, rather that of the independent action of a third party." *Murthy*, 144 S.Ct. at 1992, n.8 (cleaned up). The appellate court below

saw "no way in which [plaintiff] could, in good faith, allege that [the] loan application activity is 'fairly traceable' back to [Christie's] action." A16. It was right. Plaintiff cannot demonstrate that her claimed injury is fairly traceable to Christie's alleged conduct without engaging in rank speculation.

As with the lack of an injury-in-fact, this element of plaintiff's standing problem again begins with her complaint. Plaintiff alleges only that her publicly-available phone number and hometown were used in connection with a loan application she did not initiate. Contrary to everything she tells this Court, she does not actually allege that any of her sensitive personal information was used in the loan application or was misused in any other way. The appellate court noted that it was able to "instantly corroborate" Christie's argument that plaintiff's phone number and hometown are readily available to anyone with Internet access or the White Pages. A16, n.1. Without denying the accuracy of Christie's contention, plaintiff argues this somehow constitutes an issue of disputed fact. Pl.'s Br. 20. It does not. The Court can take judicial notice of the results of its own Google search. *See Wisnasky v. CSX Transp., Inc.*, 2020 IL App (5th) 170418, ¶ 6 (reviewing court may take judicial notice of photographs found on Google).[4] Years of litigation should not be required to answer a question that can be resolved in ten seconds.

[4] This assumes plaintiff information is not removed from search engine results before the Court reads this, in which case the Court may rely on the appellate court's representation that it verified the easy public availability of plaintiff's contact information as of the time it filed its decision. A16, n.1.

This is critical and distinguishes this case from all the authority on which plaintiff relies. As the appellate court explained, plaintiff's entire theory of the case is "purely speculative." A16. Anyone could have filled out the loan application at issue using plaintiff's readily and publicly-available phone number and hometown. Even assuming for the sake of argument that the applicant was attempting to commit fraud, "[t]here is no way, outside of speculating, for [the] court to determine that, had these hackers not breached [Christie's] e-mail, [plaintiff's] phone number and address would still not be used fraudulently" because "[t]he information would still have been public had this breach not occurred. A16. There is no authority of which Christie is aware that supports, or even suggests, that a plaintiff can prove that an injury based on the alleged misuse of non-sensitive and publicly-available information is traceable to the kind of conduct of which plaintiff accuses Christie. None.

Plaintiff argues that the appellate court's analysis was flawed because it failed to draw reasonable inferences in her favor. Pl.'s Br. 17-20. However, this argument is based on the same misrepresentations discussed above about the contents of her complaint. *Supra* 11-19. The appellate court did not fail to draw reasonable inferences in plaintiff's favor. She failed to offer well-pleaded allegations from which such inferences could reasonably be drawn.

Plaintiff also argues along these lines that circumstantial evidence can "do the job" and discovery may reveal that her Social Security number was actually used in fraudulent loan applications and there is no other known

source of exposure of her Social Security number. Pl.'s Br. 19, n.4.[5] She does not explain how discovery could answer whether her information has been part of other data breaches and, given the prevalence of data breaches and the fact that all 50 states and the District of Columbia have data breach notification laws, her argument rests on a highly questionable (if not wholly unreasonable) assumption.[6] But even if one entertains the remote possibility that plaintiff has been the victim of only one data breach, it does not change the fact that she has never actually alleged her Social Security number or other sensitive personal information was stolen in the attack on Christie and then misused, she has no apparent basis for doing so, and it is too late for her to do so for the first time now. *Supra* 15.

Plaintiff next argues that the appellate court's analysis was unduly burdensome and heightened the standard for demonstrating traceability. Pl.'s Br. 20-22. She is mistaken. Plaintiff acknowledges that Illinois' traceability requirement comes from federal law, which requires something "more than speculati[on]." Pl.'s Br. 20-21 (quoting *Parsons v. U.S. Dep't of Justice*, 801 F.3d

---

[5] Plaintiff tacitly concedes that if her information was exposed in another data breach, tying any one instance of identity theft to a specific breach would be impossible. Likewise, her argument that "temporal proximity" between the breach and the loan application can bridge the evidentiary gap (Pl.'s Br. 14, 22) fails on its face because plaintiff does not even provide approximate dates for the loan application or when she supposedly became aware of it (C85 ¶ 18).

[6] *See* Cheryl Saniuk-Heinig, *State Data Breach Notification Chart*, International Association of Privacy Professionals (March 2021), *available at* https://tinyurl.com/yy8r87af.

701, 714 (6th Cir. 2015). As discussed above, plaintiff offers nothing but speculation. It is pure speculation to assume that plaintiff's sensitive personal information was stolen from Christie—she certainly has not properly alleged it. It is pure speculation to assume that the loan application plaintiff says was an act of attempted fraud misused her sensitive personal information—she certainly has not alleged it. It is pure speculation to assume that plaintiff's publicly-available, non-sensitive information allegedly used in the loan application was illegally obtained from the attack on Christie. The list goes on, but the point is made.

In a case concerning only the alleged misuse of publicly-available, non-sensitive information, it is impossible to prove that such information was illegally obtained from one—or any—given data breach. Plaintiff therefore cannot demonstrate that her claimed injury is fairly traceable to any of Christie's supposed failings. Were the Court to find otherwise, the traceability requirement would be meaningless in data breach cases. For this reason as well, plaintiff lacks standing to sue and the dismissal of plaintiff's claims should be affirmed.

C. Plaintiff also lacks standing because her claimed injury is unlikely to be prevented or redressed by her requested relief.

Lastly with regard to standing, plaintiff claimed injury is not substantially likely to be prevented or redressed by her requested relief. *Greer*,

122 Ill. 2d at 492-93. Plaintiff alleges, without any factual support, that she has been harmed and is entitled to damages for:

> ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur…; the value of her time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

C104-05 ¶ 93. But because plaintiff only pleads an increased risk of future harm, she has no basis for requesting relief.

The Court addressed this issue in *Berry*. After holding that an increased risk of future harm is not an actionable injury, the Court further held in accordance with long-standing precedent that an "increased risk of future harm cannot alone serve as a basis for a claim for damages." 2020 IL 124999, ¶¶ 35-36 (cleaned up). The plaintiffs in *Berry* nonetheless argued that their case was exceptional because they pleaded a need for ongoing medical testing to monitor their lead levels. *Id*. ¶ 36. This Court disagreed, explaining that the plaintiff's argument was "simply another way of saying they have been subjected to an increased risk of harm. And, in a negligence action, an increased risk of harm is not an injury." *Id*. ¶ 37.

The same is true here. Plaintiff's requested damages inevitably reflect that she has not yet suffered any injury. Put simply, she seeks compensation for efforts she thinks necessary to prevent a future injury from occurring. This is exactly the kind of claim to damages rejected in *Berry*.

This is also exactly the kind of argument the Supreme Court rejected in *Clapper* and its progeny, which explains that plaintiffs cannot "manufacture standing" by taking measures to protect themselves from possible, future injuries, and then claim those measures constitute a present injury-in-fact. 568 U.S. at 415-416. Were the law otherwise, plaintiffs could unilaterally lower the bar for standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id*. at 416. As the appellate court below noted "[t]his is especially true in a case such as this, where the defendant offered free credit and identity [theft] monitoring services following the breach to mitigate" even the possibility of potential future injury. A17. Declining such a service in favor of filing a lawsuit is not self-help, it is an attempt to inflict self-harm and thereby manufacture standing.[7] For this reason as well, plaintiff lacks standing to sue and the dismissal of her claims should be affirmed.

---

[7] The appellate court in *Flores* found the defendant's offer to pay for credit monitoring following a breach served to prove "the risk of future identity theft and fraud is evident." 2023 IL App (1st) 230140, ¶ 15. As discussed above, *Flores* is distinguishable because the plaintiffs therein pleaded that they had *already suffered* fraudulent charges and the like following a breach. *Id*. *Flores* is also paradoxical because, while the appellate court found the plaintiffs there had standing, it also found they "fail[ed] to allege an adequate injury-in-fact." *Id*. ¶ 34. Regardless, the *Flores* court's reasoning flies in the face of *Berry*, *Clapper*, and common sense, creating perverse incentives for defendants like Christie to do nothing to help patients mitigate risk beyond providing notice.

III. Alternatively, plaintiff's tort claims fail as a matter of law because negligence is not a proper vehicle for her claims, and she has not suffered actual damages.

Should the Court determine that plaintiff's pleading deficiencies are not fatal to her claims, and she has standing to bring those claims, they still fail because she is attempting to use negligence as an end-run around rights and remedies specifically created by the legislature for data breach victims, and because she has not suffered actual damages.

A. The legislature created a statutory right and remedy in PIPA, making qualifying violations actionable under the Illinois Consumer Fraud Act.

Plaintiff's negligence argument asks the wrong question. The issue is not whether hospitals have a common law duty to "reasonably secure [patients'] personal and private medical information" against the risk of cyberattack. Pl.'s Br. 27, 30. They do not. No Illinois court has ever recognized such a duty. And prior to the appellate court's recent decision in *Flores*, 2023 IL App (1st) 230140, which involved a defendant (Aon) in the business of proving cybersecurity services, no Illinois court had ever created any sort of common law duty or cause of action in even arguably comparable circumstances—respectfully, it was not for the appellate court to create new law. *Hulsh v. Hulsh*, 2024 IL App (1st) 221521, ¶ 1.[8] Plaintiff all but

[8] Federal courts, including the Seventh Circuit, have generally predicted that this Court would not recognize such a duty. *See Community Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 816 (7th Cir. 2018); *In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 759-62 (C.D. Ill. 2020); *USAA v. PLS*, 260 F. Supp. 3d 965,

acknowledges this in her brief, when she admits that "no Illinois court has considered" even the first step in common law duty analysis in this context. Pl.'s Br. 30.

This is not to say that individuals actually injured by the failure to take reasonable security measures to protect sensitive personal information are without a remedy following data breaches. They have a cause of action. The legislature has enacted comprehensive legislation in PIPA spelling out, among other things: what personal information is considered sensitive and protected in Illinois (815 ILCS 530/5); who data collectors must notify in the event of a breach (*id*. §§ 12 & 15)[9]; how such information must be disposed of, providing civil penalties for improper disposal methods (*id*. § 40); and how the statute interacts with federal law (*id*. §§ 45(d), 50).

PIPA also requires data collectors that store sensitive personal information of Illinois residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45(a). And, importantly, PIPA effectively provides a remedy for its violation, stating

---

969 (N.D. Ill. 2017); *McGlenn v. Driveline Retail Merchandising, Inc.*, No. 18-cv-2097, 2021 WL 4301476, at *6-7 (C.D. Ill. Sept. 21, 2021).

[9] PIPA defines "Data Collectors" to include "privately and publicly held corporations," and "any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5.

that "[a] violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." 815 ILCS 530/20. Thus, if plaintiff can make out a claim under the Consumer Fraud Act (815 ILCS 505/1 *et seq*.), she has her remedy.

Plaintiff misses this crucial point when asking the Court to recognize a new duty in this context. So too did the appellate court in *Flores*. After finding that PIPA imposes a statutory duty by requiring data collectors to implement and maintain reasonable security measures to protect sensitive personal information, the appellate court in that case redundantly jumped into *dictum* discussing the traditional common law duty factors. *Flores*, 2023 IL App (1st) 230140, ¶¶ 23-24. In doing so, the court did not consider the distinction between statutes creating a duty and those merely establishing a standard of care. *See Valera ex rel. Nelson v. St. Elizabeth's Hosp. of Chicago*, 372 Ill. App. 3d 714, 723 (1st Dist. 2006) (discussing the distinction). More importantly, the appellate court in *Flores* did not consider the significance of the fact that the legislature, after creating the rights conferred in PIPA, then specified the remedies available, which do *not* include negligence claims. Respectfully, this was a significant flaw in the *Flores* decision—an error plaintiff now bids this Court to repeat by ignoring the intent of the legislature.

1. The Court should not second-guess the legislature's policy determination as to what remedies are available in these circumstances.

Apparently unsatisfied with this solution, plaintiff invites the Court to second-guess the legislature and recognize a new common law duty and right of action for its violation in negligence. The Court should decline that invitation.[10] The decision whether to recognize such a duty and negligence cause of action is ultimately a public policy determination. *Simpkins*, 2012 IL 110662, ¶ 17; *Charles v. Seigfried*, 165 Ill. 2d 482, 493 (1995). However, plaintiff wrongly assumes that this public policy determination should necessarily be made by the Court.

"The primary expression on Illinois public policy and social policy should emanate from the legislature." *Seigfried*, 165 Ill. 2d at 493. "This is especially true … where there is a disagreement on whether a new rule is warranted." *Id*. This Court has acknowledged that "[t]he members of our General Assembly, elected to their offices by the citizenry of this State, are best able to determine whether a change in the law is desirable and workable." *Id*. "Any decision to expand civil liability … should be made only after a thorough analysis of the

---

[10] To the extent plaintiff looks to PIPA, the FTC Act, and HIPAA as a source for finding a common law duty, her arguments fail. Neither the FTC Act nor HIPAA confer a private cause of action. *Trenton*, 887 F.3d at 816; *In re SuperValu*, 925 F.3d at 963-64; *Haywood v. Novartis Pharms. Corp*., 298 F. Supp. 3d 1180, 1191 (N.D. Ind. 2018); *Sheldon v. Kettering Health Network*, 40 N.E.3d 661, 674 (Ohio Ct. App. 2015). And Illinois courts only look to statutes as possible sources of a standard of care when they are designed to protect human life or property. *Noyola v. Bd. of Ed. of the City of Chicago*, 179 Ill. 2d 121, 129-30 (1997). Sensitive personal information is neither. *Infra* 59.

relevant considerations." *Id*. With humility and restraint, the Court has explained:

> The General Assembly, by its very nature, has a superior ability to gather and synthesize data pertinent to [an] issue. It is free to solicit information and advice from the many public and private organizations that may be impacted. Moreover, it is the only entity with the power to weigh and properly balance the many competing societal, economic, and policy considerations involved.

Id. Whereas this Court is comparatively "ill-equipped" to fashion new laws because it can consider only one case at a time and it is constrained by the facts presented (and not) before it, all of which makes it difficult to determine "the many possible permutations" that follow the creation of new law. *Id*. at 494. Moreover, the Court is generally reluctant to create new common law liability when doing so would, contrary to the stated goals of the legislature, create unlimited liability for a given form of conduct. *Id*. at 494-95.

The legislature in its wisdom determined as a matter of public policy that PIPA and the protections and remedies it affords was necessary. These rights and remedies for the protection of sensitive personal information had no common law antecedent. And in creating them, the legislature concluded that the proper recourse for those injured by inadequate data safeguarding practices lies in the Consumer Fraud Act. This balanced the goal of making relief available to those actually injured by unreasonable data security practices with the equally important goal of avoiding the creation of unlimited and potentially annihilative liability for speculative, *de minimis*, or intangible harms, especially when the defendant is itself a victim of a third party's

criminal misconduct. Private relief under the Consumer Fraud Act is limited to those who have suffered actual economic, calculable damages. 815 ILCS 505/10(a); *Morris v. Harvey Cycle & Camper, Inc.*, 392 Ill. App. 3d 399, 402 (1st Dist. 2009). For the reasons discussed above (*supra* 22-36) and below (*infra* 51-52), non-injuries like an increased risk of future identity theft do not qualify.

"Where the legislature has provided a remedy on a subject matter [courts] are not only loath but in addition harbor serious doubts as to the desirability and wisdom of implementing or expanding the legislative remedy by judicial decree." *Debolt v. Mut. of Omaha*, 56 Ill. App. 3d 111, 116 (3d Dist. 1978); *c.f. Valera*, 372 Ill. App. 3d at 723 ("it would be illogical to argue" that although the Illinois legislature has not created a private right for violation of a statute, individuals may nonetheless assert such a right "so long as [they] allege they are proceeding at common law rather than on a statutory basis"). This Court has said much the same for many years. *See*, *e.g.*, *Cunningham v. Brown*, 22 Ill. 2d 23, 29-30 (1961); *First Fed. Sav. & Loan Ass'n of Chicago v. Walker*, 91 Ill. 2d 218, 226-27 (1982); *Vancura v. Katris*, 238 Ill. 2d 352, 384 (2010). When a party is dissatisfied with a legislative policy determination, it should seek redress in the General Assembly, not this Court. *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶ 43.

Courts should thus avoid second-guessing legislative policy determinations by judicially expanding a statute's strictures. *See In re Estate of Gebis*, 186 Ill. 2d 188, 192-93 (1999) (when the legislature creates rights or

duties unknown at common law, it may limit those rights and duties and courts "must proceed within the statute's strictures"); *Walker*, 91 Ill. 2d at 226-27 (same); *Hall v. Gillins*, 13 Ill. 2d 26, 29-32 (1958) (when the legislature "created both the right and the remedy … its power to limit the maximum recovery in the action that it created can not be questioned"); *accord Morris v. Ameritech Illinois*, 337 Ill. App. 3d 40, 49 (1st Dist. 2003).

Courts should likewise respect the legislature's expressed statutory intent rather than undermine its determination by adopting and imposing new duties and remedies. *Vancura*, 238 Ill. 2d at 384. This is true even when expanding the remedies available beyond those provided for in a statute would arguably enhance its enforcement. *See Varela*, 372 Ill. App. 3d at 719-20 (rejecting argument for implied private right of action under the Abused and Neglected Child Reporting Act even if such a right would lead to enhanced enforcement); *Combs v. Ins. Co. of Illinois*, 146 Ill. App. 3d 957, 962-63 (1st Dist. 1986) (whether a statutory remedy should provide greater relief is a matter of legislative determination). After all, "the same argument could be made of almost any statute." *Varela*, 372 Ill. App. 3d at 719-20 (cleaned up).

This is not a case involving statutory ambiguity giving rise to a question of whether a private right of action should be implied therefrom. The legislature acted, creating rights and remedies under PIPA unknown to the common law, and in so doing plainly defined what is justiciable and recoverable against data collectors following data breaches. The legislature said that if

individuals are injured by unreasonable data protection practices in violation of PIPA, they must proceed under the Consumer Fraud Act. The plain language of PIPA says nothing that could be read as permitting plaintiffs to proceed under a negligence theory. That language must be read to reflect legislative intent. *See DeLuna v. Burciaga*, 223 Ill. 2d 49, 59 (2006) ("the plain language of a statute is the most reliable indication of the legislature's objectives in enacting that particular law, and when the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation") (cleaned up). When it is, the result is apparent: plaintiff cannot bring claims sounding in negligence.

Plaintiff nevertheless argues that Illinois common law already provides a duty and remedy in negligence for those whose data was compromised due to a failure to take reasonable safeguards. If this were true, there would presumably be some provision in PIPA, and some case law, saying as much. There is no indication in PIPA—none—that the legislature intended to allow those like plaintiff to bring negligence claims. The legislature saw the need to create a right and remedy when none existed and it acted. Plaintiff's apparent dissatisfaction with the legislature's solution is irrelevant. This Court has previously declined to "delv[e] in judicial metaphysics" by "say[ing] that the legislature intended to provide a remedy in addition to a common law remedy which existed but had not yet been declared by the courts." *Cunningham*, 22 Ill. 2d at 28. It should do so again. Christie thus respectfully suggests that the

Court should abide by the legislature's policy determination and thereby decline plaintiff's invitation to use the common law as an end-run around PIPA's plain language.

2. Plaintiff has not suffered actual, calculable damages and thus has no Consumer Fraud Act claim.

Further, as discussed above, private relief under the Consumer Fraud Act is limited to those who have suffered actual economic, calculable damages. 815 ILCS 505/10(a); *Morris*, 392 Ill. App. 3d at 402. By tying PIPA violations to Consumer Fraud Act actions, the legislature was plainly saying that only those who suffer actual economic damages in the wake of a data breach have a private remedy. The increased risk of future identity theft, by its very nature, does not qualify. "Without actual injury or damage, the plaintiff's claims constitute conjecture and speculation." *Cooney*, 407 Ill. App. 3d at 365 (cleaned up); *see also supra* 22-36.

The Biometric Information Privacy Act ("BIPA"), provides useful contrast. BIPA says broadly that "[a]ny person aggrieved by a violation of this Act shall have right of action in a State circuit court." 740 ILCS 14/20. Actual damages need not be alleged. *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 33. There is nothing comparable in PIPA. Indeed, by specifying that relief should be sought through the Consumer Fraud Act, and its attendant requirement for actual and calculable damages, the legislature said the opposite.

Plaintiff vaguely alleges that as a result of the attack on Christie she has non-specifically spent time, money and effort to mitigate the risk of future harm. C104-05 ¶ 93. She also seeks damages for "irrecoverable financial losses due to fraud," which she has not yet incurred, but fears she someday will. *Id*. This does not amount to calculable monetary damages. *Flores*, 2023 IL App (1st) 230140, ¶¶ 34, 42-43. Plaintiff's argument is, at its base, just another way of saying that she might be at an increased risk of future identity theft and may one day suffer harm. And, in any event, Christie offered plaintiff free credit monitoring and identity theft protections services. She cannot manufacture an injury by turning down that offer and claiming resulting damages. *See Clapper*, 568 U.S. at 415-416 (plaintiffs cannot "manufacture standing" by taking mitigation measures against speculative future injuries and thereby inflicting self-harm).

Much the same is true of plaintiff's argument that she has suffered actual damages because her personal information is property that has diminished in value as a result of the data breach. Pl.'s Br. 48. Plaintiff's information is not property. *Infra* 59. And even if it was, plaintiff offers no cognizable explanation as to how its alleged diminution could be practically valued given the fact that it has no legal market. For these reasons as well, the dismissal of plaintiff's complaint should be affirmed.

IV. Alternatively, the economic loss doctrine bars plaintiff's negligence claims.

Lastly, should the Court determine that plaintiff's pleading deficiencies are not fatal to her claims, that she has standing to bring her claims, and that the judicial creation of a new duty in negligence is proper in these circumstances, then her tort claims are nonetheless barred by the economic loss doctrine.

A. Plaintiff forfeited her challenge to the application of the economic loss doctrine.

As discussed above, after finding that plaintiff failed to state a valid claim pursuant to *Cooney*, the circuit court alternatively found the economic loss doctrine barred her negligence claims. C442. The appellate court then affirmed the dismissal of her complaint on standing grounds without addressing or disturbing this finding. A14-18. And yet plaintiff failed to raise the issue in her subsequent petition for leave to appeal. That failure has consequences.

This Court has admonished litigants appearing before it that issues not raised in a petition for leave to appeal are forfeited. *Buenz v. Frontline Transp. Co.*, 227 Ill. 2d 302, 320-21 (2008). "The fact that a party later raised the issue in its brief does not cure the forfeiture." *Crossroads Ford Truck Sales, Inc. v. Sterling Truck Corp.*, 2011 IL 111611, ¶ 62. Plaintiff's arguments in her appellant's brief challenging the circuit court's application of the economic loss doctrine in dismissing her tort claims are, therefore, forfeited. Pl. Br. 39-47.

To the extent plaintiff searches for an exception to this rule in her reply brief, Christie notes that the economic loss doctrine is not "inextricably intertwined" with other issues properly before this Court such that review would be proper. It is a separate, alternative issue, and thus subject to forfeiture. *See Lintzeris v. City of Chicago*, 2023 IL 127547, ¶¶ 42-43 (finding separate, alternative arguments are not inextricably intertwined and, as such "the forfeiture rule should be given effect").

B. The economic loss doctrine provides an independent bar to plaintiff's negligence claims.

Forfeiture aside, plaintiff's claimed losses are not recoverable in tort. As discussed above, plaintiff seeks recovery for unspecified costs she supposedly incurred mitigating the risk of future identity theft and "irrecoverable financial losses due to fraud," which she has not yet incurred, but fears she someday will. C104-05 ¶ 93. Should the court decide these are actual, well-pleaded damages, then they are surely economic losses. And purely economic losses are generally not recoverable in tort. *Moorman Mfg. Co. v. Nat'l Tank Co.*, 91 Ill. 2d 69, 88-92 (1982). Liability for purely economic losses is the province of commercial law. *In re Illinois Bell Switching Station Litig.*, 161 Ill. 2d 233, 240 (1994); *Trenton*, 887 F.3d at 812.

"Clearly, the economic loss rule applies to losses incurred without any personal injury or property damage." *In re Chicago Flood Litig.*, 176 Ill. 2d 179, 200 (1997). "Absent injury to a plaintiff's person or property, a claim presents an economic loss not recoverable in tort." *Id.* at 201. This rule has three

exceptions: "(1) where the plaintiff sustained damage, *i.e., personal injury or property damage,* resulting from a sudden or dangerous occurrence"; "(2) where the plaintiff's damages are proximately caused by a defendant's intentional, false representation, *i.e.,* fraud"; and "(3) where the plaintiff's damages are proximately caused by a negligent misrepresentation by a defendant in the business of supplying information for the guidance of others in their business transactions." *Id.* at 199 (cleaned up) (emphasis added). None of these exceptions are even arguably at play in this case.

Since its inception, the economic loss doctrine has steadily evolved. But for all its change it has remained true to its overarching goal "to prevent … open-ended tort liability." *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 418 (2004). This animating policy accounts for the fact that "the economic consequences of any single accident are virtually endless, [and] a defendant who could be held liable for every economic effect of its tortious conduct would face virtually uninsurable risks, far out of proportion to its culpability." *Id.* (cleaned up). The City argued in *Beretta* that the defendant arms manufacturer created a public nuisance by selling firearms it knew would ultimately find their way into an illegal secondary gun market. *Id.* at 362-63. The Court recognized that this scenario did not "fit neatly" within the rubric of the doctrine as previously applied, but its "concerns regarding speculativeness and potential magnitude of damages" counseled in favor of its application, and so it was applied. *Id.* at 423. The same is certainly true here.

If, for the sake of argument, one assumes that plaintiff's sensitive personal information has found its way onto the dark web, then like an illegally sold gun, it will be available for any criminal to potentially misuse. Only, in the data breach context, the potential liability is orders of magnitude greater because that information could be sold and resold, used and reused, *ad infinitum* for countless numbers of persons. The economic loss doctrine exists to cabin such speculative and unceasing liability, requiring its application here.

Plaintiff disagrees, arguing that the risk of data breach liability for hospitals is limited because it is "fully insurable." Pl. Br. 44. Her brief cites no authority for this remarkable proposition and even a cursory search of data breach insurance cases certainly suggests otherwise. *See*, *e.g.*, *Fidelity & Deposit Co. of Maryland v. Int'l Business Machines Corp.*, No. CIV. 1:05-CV-0461, 2005 WL 2665326, *3 (M.D. Pa. Oct. 19, 2005) (applying the economic loss doctrine to dismiss an insurer's negligence claim while expressing significant concerns about "valuation problems," "the nature and extent of monetary damages," and the "great" potential economic loss associated with the lost data). *Id*. Surely, there is no shortage of reported cases where insurance companies dispute their obligation to cover losses following a data breach. *See*, *e.g.*, *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, 102 F.4th 438 (7th Cir. 2024); *Citizens Ins. Co. of Am. v. Wynndalco Enterprises*, *LLC*, 70 F.4th 987, 989 (7th Cir. 2023); *Target Corp. v. ACE Am.*

Ins. Co., No. 19-CV-2916 (WMW/DTS), 2022 WL 848095, at *1 (D. Minn. Mar. 22, 2022).

The circuit court thus had it right when it concluded that plaintiff's tort claims are barred here. Numerous courts have reached the same conclusion in data breach cases. *See*, *e.g.*, *Trenton*, 887 F.3d at 817; *Perdue*, 455 F. Supp. 3d at 761 (mitigation measures following a data breach deemed economic losses subject to the economic loss doctrine); *White v. Citywide Title Corp.*, No. 18 CV 2086, 2018 WL 5013571, at *2-3 (N.D. Ill. Oct. 16, 2018) (same); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 530 (N.D. Ill. 2011) (same); *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 536 (2022), *rev. den'd* (Dec. 14, 2022); *In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009), *as am'd on reh'g in part*, (May 5, 2009) (applying Massachusetts law); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 967 (S.D. Cal. 2014) (applying Massachusetts and California law); *SELCO Cmty. Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1296 (D. Colo. 2017) (applying Colorado law); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1174 (D. Minn. 2014) (applying Iowa law).

Plaintiff nonetheless argues the economic loss doctrine applies only when the claimed losses are due to "disappointed contractual or commercial expectations." Pl. Br. 41-42. This argument seems to cut against her allegations emphasizing that Christie's Patient Privacy Policy, and related representations, create an obligation to protect her sensitive personal

information. C87; Pl.'s Br. 44 (emphasizing the parties' "direct relationship" and arguing they are not strangers). Even so, the cases discussed above demonstrate the doctrine's application is now broader than she would make it. Plaintiff also seizes upon certain phrases from several cases and statutes to cobble together a useful construct, often quoting them out of context or for misleading propositions. *Id.* at 46. This is obviously problematic. *See People ex rel. Illinois Dep't of Lab. v. E.R.H. Enterprises*, 2013 IL 115106, ¶ 29 (cautioning that care must be taken when importing definitions from other statutes without considering their context).

For instance, plaintiff argues that "most courts" now consider information lost in data breaches to be compensable property losses, pointing to a few cases applying mostly California law. Pl.'s Br. 46. The reality is that only a handful of courts have addressed this issue and at least as many have reached the opposite conclusion. *See*, *e.g.*, *Remijas*, 794 F.3d at 695, *abrogated on other grounds (supra* 35*)*; *Lewart*, 819 F.3d at 968 *abrogated on other grounds (supra* 35*)*; *Perdue*, 455 F. Supp. 3d at 762; *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 46 (D. Az. 2021); *Longenecker-Wells v. Benecard Servs. Inc.*, 658 F. App'x 659, 661 (3d Cir. 2016) (applying Pennsylvania law); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 967 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (applying Massachusetts law).

Plaintiff nonetheless insists that her sensitive personal information is property in which she has a right and thus fits within the first exception to the economic loss doctrine. Pl.'s Br. 45. Plaintiff fails to cite any relevant Illinois authority supporting this argument, and there appears to be none. If anything, this argument flies in the face of Seventh Circuit precedent, discussed above, which prior to its partial abrogation was arguably friendly to her on the standing issue, but still saw no basis for concluding that personal information is property. *See Lewert*, 819 F.3d at 968-69; *Remijas*, 794 F.3d at 695. If sensitive personal information, which has no legal market and thus cannot be legitimately bought and sold, qualifies as property, then that concept is so abstract that this exception to the economic loss doctrine swallows the rule. Tellingly, plaintiff avoids the most relevant statute, PIPA, which defines sensitive personal information, but not in terms of property. *See* 815 ILCS 530/5. One can argue that information has value, power, and other attributes. That does not make it property. For these reasons as well, the dismissal of plaintiff's complaint should be affirmed.

CONCLUSION

WHEREFORE, and for all the reasons stated above, Defendant-Appellee Christie Business Holdings, P.C., respectfully asks the Court to affirm the dismissal of plaintiff's complaint with prejudice.

Dated: August 15, 2024

Respectfully submitted,

CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRSTIE CLINIC, *Defendant-Appellee*,

/s/*Jonathan B. Amarilio*
One of Its Attorneys

Jonathan B. Amarilio
Jeffrey M. Schieber
Jaimin H. Shah
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker Drive, Suite 2600
Chicago, Illinois 60601
Tel.: 312.527.4000
jamarilio@taftlaw.com
jschieber@taftlaw.com
jshah@taftlaw.com

Attorneys for Defendant-Appellee

133793788v7

CERTIFICATE OF COMPLIANCE

The undersigned, an attorney, certifies that Defendant-Appellee's brief conforms to the requirements of Rule 341(a) and (b). The length of this brief, excluding the words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 14,999 words.

Dated: August 15, 2024

/s/ Jonathan B. Amarilio

Case No. 130337

In the
Supreme Court of Illinois

REBECCA PETTA, on her own behalf and on behalf of those similarly situated,

Plaintiff-Appellant,

v.

CHRISTIE BUSINESS HOLDINGS COMPANY, P.C., d/b/a CHRISTIE CLINIC,

Defendant-Appellee.

On appeal from the Illinois Appellate Court, Fifth Judicial District, Case No. 5-22-0742, there on appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, Case No. 22-LA-51, Hon. Jason M. Bohm, Judge Presiding

NOTICE OF FILING

TO: ***See Attached Certificate of Service***

PLEASE TAKE NOTICE that on the **15th day of August 2024**, we caused to be filed (*submitted electronically*) with the Supreme Court of Illinois, the ***Appellee's Brief***, a copy of which is hereby served upon you.

Jonathan B. Amarilio
Jeffrey M. Schieber
Jaimin H. Shah
TAFT STETTINIUS & HOLLISTER LLP
111 E. Wacker Dr., Suite 2600
Chicago, Illinois 60601
Tel.: 312.836.4042
jamarilio@taftlaw.com
jschieber@taftlaw.com
jshah@taftlaw.com

Attorneys for Defendant-Appellee

Respectfully submitted,

Christie Business Holdings Company, P.C.,
Defendant-Appellee,

By: */s/ Jonathan B. Amarilio*
One of Its Attorneys

CERTIFICATE OF SERVICE

The undersigned, pursuant to the provisions of 1-109 of the Code of Civil Procedure, and Ill. S. Ct. R. 12 hereby certifies and affirms that the statements set forth in this instrument are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be and that he caused the foregoing ***Notice of Filing*** and ***Appellee's Brief,*** to be sent to the parties listed below on this **15th day of August 2024**, by *electronic mail* from the offices of Taft Stettinius & Hollister LLP before the hour of 5:00 p.m.:

David M. Cialkowski, IL No. 6255747
Brian C. Gudmundson
Michael J. Laird
Rachel K. Tack
Zimmerman Reed LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
David.cialkowski@zimmreed.com
Brian.gudmundson@zimmreed.com
Michael.laird@zimmreed.com
Rachel.tack@zimmreed.com

Christopher D. Jennings
JENNINGS PLLC
P.O. Box 25972
Little Rock, AR 72221
Chris@jenningspllc.com

Attorneys for Plaintiff-Appellant
Rebecca Petta

/s/ Jonathan B. Amarilio

134512387v1