Case No. 130337

IN THE SUPREME COURT
OF THE STATE OF ILLINOIS

REBECCA PETTA, individually and on behalf of those similarly situated, Plaintiff-Appellant, v. CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRISTIE CLINIC Defendant-Appellee.	Petition for Leave to Appeal from the Appellate Court, Fifth District, No. 5-22-0742 Appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, No. 22-LA-51 The Honorable Jason M. Bohm, Judge Presiding

PLAINTIFF-APPELLANT'S REPLY BRIEF

David M. Cialkowski, IL Bar 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

Christopher D. Jennings
JENNINGS PLLC
500 President Clinton Avenue
Suite 110
Little Rock, AR 72221
Telephone: (501) 247-6267
chris@jenningspllc.com

Counsel for Plaintiff-Appellant Rebecca Petta

ORAL ARGUMENT REQUESTED

E-FILED
10/3/2024 8:20 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

POINTS AND AUTHORITIES

INTRODUCTION

Plaintiff-Appellant Rebecca Petta petitioned this Court for permission to appeal the Fifth District's decision affirming the trial court's dismissal of her claim. Defendant-Appellee Christie Business Holdings Co., P.C. ("Christie") asks the Court to adopt the appellate court's error. In arguing that Petta lacks standing, Christie recasts Petta's allegations to its own liking, failing to accept Petta's allegations as true or drawing reasonable inferences in her favor. Christie then sidesteps the relevant law on standing, claiming that Petta's analysis is "irrelevant" under its erroneous version of the facts.

The parties' diverging legal analyses stem from a factual disagreement: whether Petta's allegations and the reasonable inferences drawn from them allege a "fairly traceable" link between Christie's breach and a series of subsequent fraudulent loan applications using Petta's information. If, as Petta contends, they are connected, both federal and Illinois courts hold that misuse of personal information is sufficient, although not required, to establish injury-in-fact for standing. Christie does not refute that well-established law. Instead, it dismisses the misuse of Petta's data as irrelevant and claims she faces only a risk of future harm, which it wrongly contends is insufficient for standing.

The mistake Christie makes here, as the Fifth District did below, is that the role of the Court at the pleading stage is not to decide factual disagreements but to accept the well-pleaded allegations as true and draw

reasonable inferences in plaintiff's favor. Christie, under the guise of "fact pleading", demands Petta put forth definitive evidence of a link between the breach and the attempted fraud. The pleading stage does not require such definitive evidence. At this stage, courts routinely accept allegations that a breach and fraud occurring in close proximity are plausibly connected.

Here, Petta's allegations and the reasonable inferences from them support her claim that her data was stolen and subsequently misused. Petta alleged hackers accessed and successfully obtained her information during Christie's data breach and a series of fraudulent loan applications occurred after. The type of information exposed in the breach, including contact information, Social Security numbers, and other patient information, can be used to submit fraudulent loan applications. Moreover, the close timing between the two unusual events creates a reasonable inference that they are connected. Those allegations have sufficed for standing in nearly every court, including in Illinois, and should be sufficient here too.

As with standing, Christie sidesteps the key issue raised by Petta's negligence claim. Christie declines to discuss whether Petta sufficiently alleged Christie's own acts created a foreseeable risk of harm, triggering a long-established common law duty to guard against that harm. Instead, it argues Petta's negligence claim is preempted by an entirely separate claim under the Illinois Consumer Fraud Act ("ICFA") based on Christie's violation of the Personal Information Protection Act ("PIPA"). Although Christie argues

the Court should defer to the Illinois legislature, neither PIPA nor the ICFA disavow traditional common law claims or make their remedies exclusive. Christie asks the Court to infer from the legislature's silence that it intended a sweeping preemption of common law claims even though no case has found the ICFA preempts such claims or their remedies; and, indeed, ICFA claims are commonly brought with other common law claims without preemption. Such a result is also inconsistent with the purpose of both the ICFA and PIPA: to protect Illinois residents and consumers.

Finally, the parties agree that the economic loss doctrine generally applies to prevent limitless liability arising from purely economic harms. While Christie argues this is one such case, Petta asserts the opposite and courts agree. A data breach affords a limited group of individuals (those whose data was stolen) a defined set of claims (arising from inadequate data security) for a specific type of harm (the theft and misuse of the stolen data). Christie does not face unended liability to strangers, but only to its patients whose data it exposed. The economic loss doctrine does not apply here.

ARGUMENT

I. THE COURT SHOULD HOLD PETTA HAS STANDING TO BRING HER CLAIMS

Courts across the country, including in Illinois, have held that the misuse of data taken in a data breach is an injury-in-fact sufficient to bring a claim. *See Flores v. Aon Corp.*, 2023 IL App (1st) 230140, ¶ 15 (holding plaintiffs had standing because they were "not relying solely on speculative

allegations concerning an increased risk of future identity theft or fraud" but had "allege[d] that they have already experienced fraudulent charges and spam messaging."); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 773 (8th Cir. 2017) (holding that "misuse of [plaintiff's] [c]ard [i]nformation [was] sufficient to demonstrate that he had standing"); *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023) ("[A] plaintiff whose personal information is subject to a data breach can establish a concrete injury for purposes of Article III standing if, as a result of the breach, he experiences 'misuse' of his data in some way."); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 (1st Cir. 2023) ("We hold that the complaint's plausible allegations of actual misuse of [plaintiff's] stolen [personally identifying information] to file a fraudulent tax return suffice to state a concrete injury under Article III. This conclusion accords with the law of other circuits."); *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."). Here, Petta has made the same allegations those courts found sufficient—Christie experienced a data breach that caused the theft of Petta's personal and health information, and that information was subsequently used for attempted fraud. L.R. C197 V2, ¶¶ 18–19.

Christie does not refute the law but contends Petta's allegation of a connection between the breach and the fraud are not reasonable.[1] Appellee's Br. ("Def. Br."), at 12. No court has required the degree of proof at the pleading stage Christie would impose here. *See SuperValu*, 870 F.3d at 772 (holding that "[a]t this stage of the litigation, we presum[e] that [these] general allegations embrace those specific facts that are necessary to support a link between the . . . fraudulent charge and the data breaches." (internal quotations removed)); *Webb*, 72 F.4th at 374 (holding that "[t]here is an obvious temporal connection between the filing of the false tax return and the timing of the data breach" and "the obvious inference to be drawn from th[e] allegations is that the criminal or criminals who file the false tax return obtained [plaintiffs' information] from the . . . data breach[.]").

As described further below, Petta adequately alleged that her data was stolen and subsequently misused. The Court should reject Christie's attempt to transform the standing inquiry into one evaluating a threat of future harm because Petta has adequately alleged she already suffered harm.

A. Fraud After a Data Breach is Undisputedly Sufficient to Establish an Injury in Fact

Contrary to Christie's argument, courts widely hold that data breach victims have standing to bring their claims even if no misuse of the data has

[1] If the issue of standing comes down to the sufficiency of Petta's allegations, she should be allowed to amend. While Christie argues it is too late to amend, the trial court did not allow amendment because it believed key legal issues needed to be resolved on appeal. L.R. C463 V2.

occurred, particularly where the hacker succeeded in obtaining sensitive data. *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153–54 (3d Cir. 2022) (holding "misuse is not necessarily required" for standing and providing factors considered when establishing whether the risk of harm establishes standing); *In re U.S. Office of Personal Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42 (D.C. Cir. 2019); *In re Netgain Tech. Customer Data Breach Litig., LLC*, No. 21-cv-1210, 2022 WL 1810606, at *5 (D. Minn. June 2, 2022) ("Other circuits have held that there is a substantial risk of future harm when [sensitive information] is stolen" and collecting cases").

Federal appellate courts agree, however, that an allegation of the misuse of the data stolen in a data breach establishes standing. *See, e.g.*, *SuperValu*, 870 F.3d at 773; *Green-Cooper*, 73 F.4th at 889; *Webb*, 72 F.4th at 373; *Attias*, 865 F.3d at 627. Illinois courts have held the same. *See Flores*, 2023 IL App (1st) 230140, ¶ 15; *Maglio v. Advoc. Health & Hosps. Corp.*, 2015 IL App (2d) 140782, ¶¶ 28–29.

In *Maglio*, for example, the court compared standing in the case before it, where no misuse of data had occurred, to those alleging misuse. 2015 IL App (2d) 140782, ¶¶ 28–29. The court noted that plaintiffs would have standing if they alleged "fraudulent activity, such as attempted access to bank accounts and opened cell phone accounts" following the breach. *Id.* (citing *Tierney v. Advoc. Health & Hosps. Corp.*, No. 13-cv-6237, 2014 WL 578333, *2 (N.D. Ill. Sept. 4, 2014)). However, the *Maglio* plaintiffs lacked standing because they

had not alleged any misuse of their information or a real threat of future harm, as they alleged the theft of a laptop with no evidence the thief sought the personal information contained within it. *Id.* ¶ 29.

Under both federal and Illinois law, the misuse of data after a data breach establishes standing. Petta, here, alleged both requirements necessary to meet this standard. She alleged her information was taken in the breach. *See* L.R. C216 V2, ¶ 89 ("Hackers successfully breached Defendant's network and data environments, resided there undetected for more than a month, and stole a host of personal and healthcare information on hundreds of thousands of Christie Clinic's patients."); C216, ¶ 92 ("But for Christie Clinic's wrongful and negligent breach of its duties, her [s]ensitive [i]nformation would not have been accessed and exfiltrated by unauthorized persons."). Additionally, she alleged subsequent misuse of her data in a series of fraudulent loan applications. *Id.* C197 V2, ¶ 18 (alleging she received a call from a bank in Ohio that received several loan applications using her information); C213 V2, ¶ 76 ("Plaintiff's [personally identifying and health information], like that of every other Class member, was misused and improperly disclosed by Defendant."); C195 V2, ¶ 8 (alleging that, prior to notice, hackers had the opportunity to misuse this information without Christe Clinic's patients' knowing or having the opportunity to implement measures to protect themselves."). This is sufficient for standing in federal court and under Illinois precedent.

Chistie asks the Court to ignore that misuse because it supposedly only included non-sensitive information. Def. Br. at 38. That argument misses the importance of the misuse of the data exposed in a breach.

That Petta experienced fraud so close to Christie's data breach provides a reasonable inference about the scope the breach: the data at issue was not merely exposed, it was taken. The hacker that breached Christie and resided there undetected for more than a month successfully took her data. *See Green-Cooper*, 73 F.4th at 889 (noting that "misuse of the data cybercriminal acquired from a data breach" is evidence of a "'substantial risk' of harm in the future"); L.R. C195 V2, ¶ 6. As Christie acknowledged, that hacker had access to Petta's sensitive information, including her name, address, Social Security number, dates of birth, medical history, and medical insurance information. L.R. C197 V2, ¶ 18. The hackers use of at least some of the data suggests it has it all.

For that reason, several courts have found standing even where the misuse only partially included the data exposed in the breach. *See Flores*, 2023 IL App (1st) 230140, ¶ 16 (rejecting defendant's argument that because they did not "collect[] payment information . . . [plaintiffs] ha[d] not established that the unauthorized charges . . . [were] fairly traceable to defendant's conduct and the data breach" and recognizing that data can be "package[d] with personal information" and "sold to third parties to be later used for illicit purposes."); *In re Mednax Servs., Inc. Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1206 (S.D. Fla. 2022) ("Even if the data accessed in the [d]ata [b]reaches did

not provide all the information necessary to inflict these harms, they very well could have been enough to aid therein.").

The misuse of Petta's information for fraudulent loan applications so soon after the data breach shows the hacker sought out and took Petta's data from Christie and used it for fraud or sold it to fraudsters. L.R. C195 V2, ¶ 6. That is enough for standing in nearly all, if not all, courts across the country. The Court should find is sufficient under Illinois law here.

B. The Misuse of Petta's Personal Information is "Fairly Traceable" to the Data Breach

To establish standing, the injury must be "fairly traceable" to the wrongdoing alleged. *Greer v. Illinois Housing Dev. Auth.*, 122 Ill. 2d 462, 492 (1988). While Christie and Petta may draw different inferences from the facts of the data breach—just as did the Fifth District and trial court did—Petta has adequately alleged the misuse of her data in fraudulent loan applications is fairly traceable to the Christie's misconduct and the resulting breach.[2]

Courts recognize that "'fairly traceable' does not mean 'certainly traceable.'" *See Mednax*, 603 F. Supp. 3d at 1205–06. "This traceability requirement does not mean a plaintiff must show to a scientific certainty that defendant . . . caused the precise harm suffered." *McCreary v. Filters Fast LLC*,

[2] Christie claims the Court should reconsider its granting of Petta's petition for leave to appeal because Petta supposedly misrepresented her complaint. She did not. As described below, her allegations and the reasonable inferences therefrom establish a connection.

No. 3:20-cv-0595, 2021 WL 3044228, at *5 (W.D.N.C. July 19, 2021) (internal quotations omitted)).

In the context of a data breach, courts routinely recognize that fraud occurring soon after a data breach is, at least at the pleading stage, fairly connected. *See Webb*, 72 F.4th at 374; *Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-0036, 2023 WL 6383467, at *6 (S.D. Ohio Sept. 29, 2023) ("While [p]laintiffs do not explicitly allege that the data breach 'caused'" certain misuse of the data, "their point is clear—the increase is traceable to the data breach. . . . Plaintiffs need not *prove* that the data breach caused the [misuse]" because "it is more than a 'sheer possibility' that a data breach involving contact information would lead to [misuse]."); *SuperValu*, 870 F.3d at 772 (holding allegations that "customer [c]ard [i]nformation was stolen by the hackers" and that plaintiff "became the victim of identity theft after the data breaches" adequately stated a "causal connection").

Although federal courts treat the traceability standard leniently, especially at the pleading stage, Christie claims this Court should demand more. In its view, Illinois's fact-based pleading standard requires her to disprove the possibility that a different source for her personal information was used to submit the fraudulent loan applications.

To reasonably infer a connection between the breach and the fraud, however, Petta is not required to eliminate all other possible sources for the misused data. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 969

(7th Cir. 2016) ("Merely identifying potential alternative causes does not defeat standing."); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015) ("The fact that . . . [a breach of] some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate plaintiffs' standing to sue." (emphasis in original)); *Huynh v. Quara, Inc.*, 508 F. Supp. 3d 633, 651 (N.D. Cal. 2020) ("[T]he mere fact that Plaintiff has been a victim of other more serious breaches in the past does not mean a substantial connection . . . is lacking."); *S. Indep. Bank v. Fred's, Inc.*, No. 2:15-cv-799, 2019 WL 1179396, at *8 (M.D. Ala. Mar. 13, 2019) ("Plaintiff is not required to eliminate entirely all possibility that [defendant's] conduct was not the cause of its damages." (internal quotations omitted)).

At the pleading stage, "[t]he critical inquiry is whether the allegations of the complaint, when construed in the light most favorable to the plaintiff, are sufficient to establish a cause of action[.]" *Kanerva v. Weems*, 2014 IL 115811, ¶ 33. A court does not decide parties' factual disputes, particularly where a defendant's assertion contradicts the allegations of the complaint. *See Kahn v. Deutsche Bank AG*, 2012 IL 112219, ¶ 49 ("[W]e bear in mind that we are not determining whether a fiduciary relationship actually existed" but "only whether . . . the well-pleaded factual allegations of the complaint adequately alleged that a fiduciary duty existed"). Rather, a "court must accept as true all well-pleaded facts in the complaint, as well as any reasonable inferences that may arise from them." *Kanerva*, 2014 IL 115811, ¶ 33. The

complaint should not be dismissed "unless it is clearly apparent from the pleadings that ***no set of facts*** can be proven that would entitle the plaintiff to recover." *Id.* (emphasis added).

Here, Petta's allegations support the reasonable inference that the attempted fraud and Christie's data breach are connected. She alleged that cybercriminals routinely target healthcare clinics because patient data has significant value on the dark web through its sale to fraudsters. L.R. C205–06 V2, ¶¶ 51–56. For over a month in 2021, a hacker breached a Christie email account and had access to thousands of patients' names, addresses, Social Security numbers, medical information, and health insurance information. *Id.* C199–200 V2, ¶¶ 28–29. Christie's investigation of the breach concluded the hacker was financially motivated. *See id.* C226 V2 (describing the hackers attempt to intercept a transaction between Christie and a vendor). Moreover, Christie notified its patients that their personal and patient information were at risk due to the breach, and that its investigation could not rule out that such data was taken for all impacted patients. *Id.* ("Christie Clinic and our professional forensic investigators have concluded that the extent of the access is unknown and cannot be determined.").

Shortly after the data breach, Petta experienced a series of fraudulent loan applications filled out using her information. She alleges that one fake loan application included *at least* her phone, city, and state. *Id.* C197 V2, ¶ 18. While she does not know the full extent of the misuse, loan applications

typically require sensitive information, including Social Security numbers—which were exposed in this breach—to conduct credit checks. Moreover, Christie warned its patients of the possibility of this exact type of fraud based on the data that was compromised and provided monitoring tools to detect that fraud. *See id.* C227 V2 (warning patients to "remain vigilant against incidents of identity theft and fraud[.]"). Given those allegations, the close timing between the breach and the fraud, and that the information exposed in the breach could be used to submit fraudulent loan applications, Petta has alleged enough at this early stage to show the reasonable inferences, when drawn in her favor, meet the traceability standard.

Unsurprisingly, Christie attempts to draw different inferences from those same facts than Petta draws about the hacker's motive and the connection between the breach and the fraud. At this stage though, those inferences are drawn in Petta's favor. She has put forth sufficient allegations to show the fraud is "fairly traceable" to Christie's misconduct and the breach.

C. Petta's Injuries are Redressable

Christie also argues Petta's injuries are not redressable, again relying on the notion that Petta has not adequately alleged the fraudulent loan attempts are connected to the breach. "[T]he injuries caused by a data breach are easily and precisely compensable with a monetary award[.]" *Clemens*, 48 F.4th at 158 (internal quotations omitted); *see also Webb*, 72 F.4th at 377 (holding that data breach victims' harms could be redressed by the court

because "monetary relief would compensate [the plaintiffs] for their injur[ies], rendering the injur[ies] redressable." (internal quotations omitted)). Here, the harm Petta incurred responding to the data breach and the loss in the value of her personal information may be redressed with a monetary award, satisfying the redressability requirement.

II. PETTA ADEQUATELY PLED HER NEGLIGENCE AND ICFA CLAIMS

Petta brought claims against Christie for common law negligence and under the ICFA for Christie's violation of PIPA. Christie contends Petta's negligence claim is preempted by the availability of an ICFA claim and, further, that Petta has not established "actual damages" necessary to bring an ICFA claim. The Court should reject both arguments.

A. Petta's Negligence Claim Arises Under Illinois Common Law

Petta's negligence claim is based on Illinois' "long recognized" common law rule that one should not take actions that impose a foreseeable risk of harm to others. *See Simpkins v. CSX Transp., Inc.*, 2012 IL 110662, at ¶ 19 ("[I]f a course of action creates a foreseeable risk of injury, the individual engaged in that course of action has a duty to protect others from such injury."). To determine whether the "long-recognized" duty applies, courts consider whether: (1) "the defendant, by his act or omission, contributed to a risk of harm to this particular plaintiff", *id.* ¶ 21; and (2) the four public policy factors establish a sufficient relationship between the parties to find a duty, *see id.* ¶

18 (explaining that the "relationship" requirement "acts as a shorthand description for the sum of the four factors[.]").

While Petta applies that duty in the data breach context, that does not make this duty new. *Id.* ¶ 19 (holding "this court has long recognized" the duty to guard the foreseeable risk of harm that flows from one's acts). As the Pennsylvania Supreme Court held in applying its common law duty in a data breach case, "this case is one involving the application of an existing duty to a novel factual scenario, as opposed to the imposition of a new, affirmative duty[.]"). *Dittman v. UPMC*, 649 Pa. 496, 512 (Pa. 2018); *see also Netgain*, 2022 WL 1810606, at *11 (holding that a data breach case was "a general negligence case where [defendant's] own conduct, in failing to maintain appropriate data security measures, created a foreseeable risk of harm that occurred[.]").

Here, Petta alleged that Christie's conduct created a foreseeable risk of harm to her and, further, that the four public policy factors support finding a duty. Consistent with *Dittman*, Petta does not assert this duty is an affirmative one existing every time data is lost. Rather, Petta has recognized that certain data disclosures may not trigger this duty because, for example, the disclosure is unforeseeable or accidental. *Compare Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358, 360 (2010) (finding no duty in an unforeseeable, accidental disclosure to non-criminals),[3] *with Flores*, 2023 IL App (1st) 230140, ¶ 24

[3] The *Cooney* court evaluated only whether an affirmative duty arose from statute, not whether the defendant's own acts created a foreseeable risk of harm. *See id.* at 361–62. As *Flores* correctly found, *Cooney's* reasoning no

(finding a duty where defendant employed inadequate security it knew or should have known created the risk of a data breach). Here, Petta alleges Christie knew it was a target for data thieves and employed unreasonably deficient data security anyway, putting her at a foreseeable risk of harm. L.R. C205 V2, ¶ 53.

Neither Christie nor Amicus dispute that the public policy factors support finding a claim here. Christie, instead, argues Petta's common law claims are entirely preempted by the availability of an ICFA claim.[4] As described below, Petta's claim is not preempted.

B. The Availability of an ICFA Claim Does Not Preempt Petta's Negligence Claim

Although no court appears to have held so before, Christie argues that the availability of an ICFA claim preempts all other common law claims and remedies. A violation of PIPA "constitutes an unlawful practice under the [ICFA]." 815 ILCS 530/20. The ICFA affords a right of action to those who suffer "actual damages" due to unfair, deceptive or unlawful practices. 815 ILCS 505/10a. Christie claims, through PIPA, the legislature abolished all

---

longer applies due to the legislature's amendments of PIPA requiring reasonable security. *Flores*, 2023 IL App (1st) 230140, ¶¶ 21–23.

[4] Amicus separately argue that PIPA does not support finding a common law duty, an argument that confuses Petta's separate claims. Her negligence claim is based on a duty that arose because Christie's actions created a foreseeable risk of harm and her ICFA claim is based on a violation of PIPA's requirement that Christie implement reasonable data security.

other common law claims and data breach victims' only remedy is through the ICFA. PIPA does not support such sweeping preemption.

"[T]he mere existence of a statute establishing legal duties . . . does not foreclose the possibility of a common law negligence action based on an extra-statutory duty of care." *Vancura v. Katris*, 238 Ill. 2d 352, 377 (2010). The court has explained that "where the legislature enacts a statute establishing a means to enforce existing rights, there is no presumption that the statutory means is intended either as exclusive remedy or to abolish other actions at common law or equity[.]" *Jackson v. Callan Pub., Inc.*, 356 Ill. App. 3d 326, 336 (2005) (emphasis removed).

For a statute to abolish all common law claims, the legislature must "express or manifest the intent to give the statute such a preemptive effect." *Id.* "[W]here there are no negative words or other provisions making the new remedy exclusive, it will be deemed to be cumulative only and not intended to take away prior remedies." *Kosicki v. S.A. Healy Co.*, 312 Ill. App. 307, 315 (Ill. App. Ct. 1941), *aff'd* 380 Ill. 298 (1942) (rejecting defendant's claim that "the exclusiveness of the new [statutory] remedy may appear by implication").

Here, Christie claims that the mere enactment of PIPA abolished all traditional common law claims for data breach victims in favor of an ICFA claim. Def. Br. 43–44. Yet, such stern language is found nowhere in the statute. PIPA contains no "negative words" disavowing common law claims nor any statement that an ICFA claim affords data breach victims their sole remedy.

Kosicki, 312 Ill. App. at 315; *see also Jackson*, 356 Ill. App. 3d at 336 ("Nothing in this Act or its legislative history indicates that it is intended to be the sole remedy under the circumstances here."); *Vancura*, 238 Ill. 2d at 377 ("A statute will be construed as changing the common law only to the extent the terms thereof warrant, or as necessarily implied from what is express." (quotations omitted)).

Moreover, although ICFA claims are commonly brought with common law claims, Christie does not cite a single case holding that the availability of an ICFA claim preempts all other claims or limits the remedies available under them. Such a result would be at odds with the purpose of the ICFA and PIPA to protect consumers. *See Robinson v. Toyota Motor Credit Corp.*, 201 Ill. 2d 403, 416 (2002) (describing the ICFA as "a regulatory and remedial statute for the purpose of protecting consumers and others against fraud, unfair methods of competition, and unfair or deceptive acts or practice."); *see also* 815 ILCS 530/45(a) (requiring "reasonable security measures *to protect* [individuals'] records" containing personal information (emphasis added)).

The Court should decline to hold that the legislature silently preempted all common law claims related to data security by enacting PIPA. The better view is that the legislature intended PIPA to supplement the remedies available to data breach victims under the common law by treating unreasonable data security as an unlawful practice under the ICFA. *See Kosicki*, 312 Ill. App. at 314 (holding that the statutory remedies "will be

deemed to be cumulative only and not intended to take away prior remedies" absent express language). Consequently, Petta's negligence claim (arising from the long-established duty not to take actions that put others at foreseeable risk) and her ICFA claim (arising from Christie's violation of PIPA) are separately actionable claims.

C. Petta Alleged Actual Damages Sufficient to Bring her ICFA Claim

Christie contends that Petta has not suffered actual damages, as required to bring an ICFA claim. Def. Br. 51–52. However, Petta directly alleged an actual loss in the value of confidential information by its public disclosure in Christie's breach.

No different than a company's trade secret, Christie's data breach impaired the value of Petta's data by eliminating its confidentiality and making that private information public. That is the very harm PIPA recognizes that data breaches cause to their victims. *See* 815 ILCS 530/5 (defining a data breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information").

While Christie asserts there is no feasible means of measuring the value of the data, the value can be measured in both legal markets, where personal information is bought and sold by advertising companies, and illegal ones, where criminals purchase this information on the dark web. L.R. C206 V2, ¶ 54–55. Moreover, studies have expressly measured the amount consumers would pay to keep their information private, a direct measure of the value lost

when Petta's private information was taken by cybercriminals. *See id.* C206–07, ¶ 56 (alleging consumers would pay between $30.49 and $44.62 to protect against improper access and secondary use of personal information). Petta, thus, alleged "actual damages" and may bring her ICFA claim.

III. THE ECONOMIC LOSS DOCTRINE DOES NOT BAR PETTA' S NEGLIGENCE CLAIM

Christie argues that the Court should not consider the economic loss doctrine because Petta supposedly forfeited that issue. It also claims that the economic loss doctrine bars Petta's tort claim due to the threat of limitless liability. The Court should reject both arguments.

A. Petta Has Not Forfeited Consdieration of the Important Issue of the Economic Loss Doctrine

Christie claims Petta forfeited consideration of the economic loss doctrine by failing to raise it in her petition for leave. However, the economic loss doctrine is integral to the question of whether data breach victims may bring common law tort claims, one of the primary issues in Petta's petition. *See* Pet. at 1 (seeking "guidance on the important issue of the merits of certain tort and statutory claims arising in the context of a data breach.").

Also, where "an issue [that] is not specifically raised in a party's petition for leave to appeal" is "'inextricably intertwined' with other matters properly before the court, review is appropriate." *Lintzeris v. City of Chicago*, 2023 IL 127547, ¶ 42. Here, the economic loss doctrine is "inextricably intertwined" with the issue of whether data breach victims may bring a common law tort

claim because, if applied, the economic loss doctrine would bar such claims. Without guidance from this Court, courts are likely to continue to be divided on the application of the doctrine to these cases. *See, e.g.*, L.R. C442 V2 (order by the Trial Court applying the economic loss doctrine); *Flores*, 2023 IL App (1st) 230140, ¶¶ 57–58 (declining to apply the doctrine).

Lastly, the Court may consider a relevant issue regardless of the petition if it is "one of law, the issue is fully briefed and argued by the parties, and the public interests favors considering the issue." *Lintzeris*, 2023 IL 127547, ¶ 42. Here, the parties fully briefed the issue, and it is necessary to resolve the viability of Petta's and other data breach victims' tort claims. The Court should consider it.

B. The Economic Loss Doctrine Does Not Apply Here

In Illinois, the economic loss doctrine acts as an arrow that points plaintiffs to the proper vehicle for their claims (*i.e.*, contract or tort) or a yardstick that ensures a sufficient connection between the wrongdoer and the plaintiff (*i.e.*, to prevent limitless liability). Here, neither purpose is served. Christie's duties do not arise out of contract. *See Congregation of the Passion v. Touche Ross & Co.*, 159 Ill. 2d 137, 162 (1994) ("Where a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty."); *Flores*, 2023 IL App (1st) 230140, ¶ 57. Additionally, as discussed below, Christie would not be subject to limitless liability.

Christie likens this case to *City of Chicago v. Beretta U.S.A. Corp.*, where the Court's concerns of limitless liability caused it to apply the economic loss doctrine to a governmental agency's lawsuit against gun manufacturers concerning their role in increasing gun violence in Illinois. 213 Ill. 2d 351, 357–363 (2004). Christie claims that, like a gun being released into Illinois communities, the theft of private data can be used in innumerable ways to cause harm and, therefore, it would supposedly be subjected to limitless liability. Def. Br. at 55. This analogy is inappropriate.

As both Petta and Christie acknowledge, Illinois courts have used the economic loss doctrine to prevent defendants from being subject to liability for harms far removed from its misconduct. *See Beretta*, 213 Il. 2d at 418 (describing the "policy underlying the economic loss rule" is to prevent liability for "every economic effect of its tortious conduct."). This Court noted that, without the economic loss doctrine, liability may attach even where the parties are "'strangers'" with "'no foreknowledge of each other's activities[.]'" *Id.* at 423 (quoting *In re StarLink Corn Prods. Liab. Litig.*, 212 F. Supp. 3d 828, 842 (N.D. Ill. 2002)). The Court's concern in those cases is that defendants would be liable to unknown and unidentified plaintiffs (*i.e.* strangers) far down the causal chain from its initial wrongdoing.

This case poses no such risk. Christie would not be liable to "strangers" for its data breach, but rather, to a specific and limited number of its own, identifiable patients whose data it collected and exposed to a cybercriminal.

See, e.g., *Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 594 (S.D.N.Y. 2022) (finding defendant did not face "limitless liability" because liability was limited "to the individuals whose personal information it obtained while providing its services."). Christies, in fact, is aware of the number and identity of all these potential plaintiffs, as it sent each a notice of the data breach after its investigation.

In *Beretta*, creating liability for gun manufacturers for an increase in gun violence meant an endless number of potential *plaintiffs* could bring claims. The *Beretta* plaintiffs sought to hold gun manufacturers liable for the economic harm incurred mitigating the increase in crime and gun violence, which would, if successful, open gun manufacturers to potential liability from a limitless number of strangers with whom it has no knowledge or relationship. The theft and sale of personal data (even the repeated sale of that data) on the dark web does not subject Christie to liability to any new or additional *plaintiffs*. The potential plaintiffs remain those patients Christie notified as having data exposed in the breach. At most, the release of the data on the dark web may impact the damages calculations, but it does not increase Christie's liability to any additional people or entities.

Further, Petta's harm is far more connected to the wrongdoing than in *Beretta*. The data breach resulted in the physical extraction of Petta's private information from Christie's computers and its subsequent use on loan applications. Her damages are directly tied to a definable good—the misuse of

her data. *Beretta*, by contrast, involved economic compensation for a wide range of harms related to public health and safety that were far removed from the initial wrongdoing, the illicit sale of a gun. *See* 213 Ill. 2d at 361–62. This case is far more akin to those cases where the economic loss doctrine does not apply because the harm involved damage to a tangible property than it does to the line of cases applying the doctrine to prevent limitless liability to strangers.

The Court should decline to apply economic loss doctrine to Petta's claims.

CONCLUSION

The Court should reverse the Fifth District opinion and reinstate Petta's negligence and ICFA claims.

Dated: October 3, 2024

/s/ David M. Cialkowski
David M. Cialkowski, IL No. 6255747
Brian C. Gudmundson
Michael J. Laird (*Pro hac vice*)
Rachel K. Tack
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
david.cialkowski@zimmreed.com
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher Jennings
JENNING PLLC
P.O. Box 25972
Little Rock, AR 72221
Telephone: (501) 247-6267
chris@jenningspllc.com

Attorneys for Plaintiff-Appellant Rebecca Petta

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or 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, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 5,978 words.

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

Dated: October 3, 2024

/s/ David M. Cialkowski
David M. Cialkowski

Attorney for Plaintiff-Appellant

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2024, I electronically filed Plaintiff-Appellant's Reply Brief with the Clerk of the Supreme Court of Illinois using an approved Electronic Filing Service Provider ("EFSP"). I further certify that a copy of the same was served via electronic mail upon the following:

Jonathan B. Amarilio
Jaimin H. Shah
Taft Stettinius & Hollister LLP
111 E. Wacker Drive, Suite 2600
Chicago, IL 60601
jamarilio@taftlaw.com
jshah@taftlaw.com

Jeffrey M. Schieber
Nelson Mullins Riley & Scarborough LLP
123 N. Wacker Drive, Suite 2100
Chicago, IL 60606
jeff.schieber@nelsonmullins.com

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

Dated: October 3, 2024

/s/ David M. Cialkowski
David M. Cialkowski

Attorney for Plaintiff-Appellant