STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT IV

Alp Baysal, Sandra Italiano, Thomas Maxim and Robert Park,

Plaintiffs-Appellants,

v. Appeal No. 2024AP001510

American Family Life Insurance Company, Midvale Indemnity Company and American Family Mutual Insurance Company, S.I.,

Defendants-Respondents.

On Appeal from the Circuit Court of Dane County
The Honorable Nia Trammell, Circuit Court Judge, Presiding
Circuit Court Case No. 2023CV002942

BRIEF OF PLAINTIFFS-APPELLANTS ALP BAYSAL, SANDRA ITALIANO, THOMAS MAXIM, AND ROBERT PARK

Jessica N. Servais (WI # 1048014)
Kate M. Baxter-Kauf (admitted *pro hac vice*)
Karen Hanson Riebel (admitted *pro hac vice*)
Maureen Kane Berg (admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Attorneys for Plaintiffs-Appellants

Additional Counsel Identified in Signature Block

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF THE ISSUES PRESENTED

OVERARCHING ISSUE I: Did the Trial Court err by ruling that Plaintiffs lacked standing to bring this case in the Wisconsin State Courts?

ISSUE A: Did the Trial Court err by failing to apply the Wisconsin Court of Appeals' binding precedent on standing in the data breach context, as set forth in *Reetz v. Advocate Aurora Health, Inc.*, 2022 WI App. 59, 405 Wis. 2d 298, 983 N.W.2d 669 (Wis. App. 2022)?

Sub-Issue 1: Did the Trial Court err by denying that the unemployment fraud Defendants predicted, and Plaintiffs experienced, was harm to the Plaintiffs and was plausibly tied to the Data Disclosures?

Sub-Issue 2: Did the Trial Court err by denying that the fraudulent financial accounts opened in Plaintiffs' names were harm to the Plaintiffs and were plausibly tied to the Data Disclosures?

ISSUE B: Did the Trial Court err by recycling the federal courts' Article III jurisdictional standing analysis, which does not apply in state court and certainly does not overturn *Reetz*?

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

Plaintiffs request oral argument and publication of the Court's opinion under Wis. Stat. §§ 809.19(1)(c) and 809.23(1)1. and 5., because this Court's opinion will clarify existing rules regarding the meaning of "standing" in Wisconsin state courts and will distinguish those rules from the jurisdictional rules regarding "Article III standing" that apply in federal courts. The opinion will also clarify the application of Wisconsin state court "standing" rules in the data breach context. Such clarifications will be of substantial and continuing public interest.

STATEMENT OF THE CASE

A. Introduction and Procedural Background.

In February 2021, at the height of the pandemic, the New York State Department of Financial Services ("NYDFS") issued an industry letter to insurance

companies alerting them to "a systemic and aggressive campaign to . . . steal unredacted drivers' license numbers [from insurers' instant quote websites, and that], at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits." App. B39, ¶ 97, n. 46.[1] NYDFS had learned from two auto insurers that cybercriminals were targeting their websites to obtain unredacted drivers' license numbers as part of a growing fraud campaign targeting pandemic and unemployment benefits and so the NYDFS alerted the entire industry to the problem. *Id.*

Insurers' instant online auto quoting websites were the primary entry point for cybercriminals to access consumers' PI. App. B48, ¶ 98. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and then captured the full, unredacted drivers' license numbers without going any further in the process and abandoned the quote. *Id.* Drivers' license numbers are protected information under the Drivers' Privacy Protection Act t ("DPPA"), 18 U.S.C. §§ 2721, 2724 and insurers may obtain, use, or disclose them only for limited purposes under the Act – mostly to verify identities for underwriting purposes. Of course, insurers need not use drivers' license numbers on a sales platform, or disclose this information to the public, to underwrite any auto insurance policy, but several insurers, including Defendants, had added a "pre-fill" feature to their instant quote platforms in order to increase their sales, thus disclosing unredacted drivers' license numbers to anyone who entered a bare minimum of publicly available information about that individual. App. B7-B8,B40, ¶¶ 8-10, 98.

Several insurers were caught up in this scheme by which malicious actors obtained protected drivers' license numbers from their instant quote websites and used them to commit unemployment and pandemic benefits fraud and other identity

[1] All references to "App. ___" are to Plaintiffs-Appellants' Appendix, filed herewith. Where, as here, the reference is to the Complaint (Doc. 4; "App. B"), Plaintiffs include the paragraph number for ease of review.

theft, including the three Defendants here: Midvale Indemnity Company ("Midvale"), American Family Insurance Company, S.I. ("AmFam"), and American Family Life Insurance Company ("AFLIC") (collectively "American Family" or "Defendants"). Other insurers who disclosed protected drivers' license numbers on their instant quote websites included GEICO, Travelers, USAA, and Farmers. App. B33-B35, ¶¶ 79, 83; *See, e.g.*, *In re GEICO Customer Data Breach Litig.*, No. 21-CV-2210-KAM-SJB, 2023 WL 4778646, at *12-14 (E.D.N.Y. July 21, 2023), *report and recommendation adopted*, 2023 WL 5524105 (E.D.N.Y. Aug. 28, 2023); *Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55, 68 (S.D.N.Y. 2022); *In re USAA Data Security Litig.*, 621 F. Supp. 3d 454, 458 (S.D.N.Y. Aug. 12, 2022); *Stallone v. Farmers Group, Inc.*, No. 221CV01659GMNVCF, 2022 WL 10091489, at *10 (D. Nev. Oct. 15, 2022). After members of the public experienced a variety of identity theft following this "systemic campaign," including fraudulent unemployment applications and fraudulent financial accounts opened in their names, many of them brought suits against this array of insurers who had disclosed their drivers' license numbers to cybercriminals and enabled that fraud.

The American Family Defendants were particularly egregious insurers, because they permitted a series of three separate Data Disclosures on their instant quote websites. App. B9-B11, ¶¶15-18. Plaintiffs Baysal, Italiano, and Maxim brought suit for the first two Data Disclosures (against Midvale and AmFam). App. B15, ¶38. Almost a year later, AFLIC enabled the third Data Disclosure by the very same mechanism, and Plaintiff Park brought suit. *Id.*

While several federal district courts around the country have found standing under these circumstances and litigation has proceeded against GEICO, USAA, Travelers, and Farmers, the federal courts hearing the cases against the American Family Defendants decided they lacked jurisdiction under Article III of the U.S. Constitution and dismissed these cases without prejudice, and without any evaluation of the merits. *Id.* Plaintiffs therefore re-filed their (now consolidated) case in Wisconsin state court, where Article III of the U.S. Constitution does not

apply. App. B1-B84. The Trial Court failed to apply the Wisconsin Court of Appeals' binding precedent setting forth the application of state court "standing" principles in the data breach context, and instead wrongly restated and reapplied the reasoning of the federal courts and dismissed the case for lack of standing. App. A1-A16.[2] Plaintiffs timely filed their notice of appeal. App. C1.

B. Disclosure of consumers' private information, including drivers' license numbers, leads to increasing identity theft.

As Plaintiffs' Complaint alleges, every year millions of Americans have their most valuable personal information ("PI") accessed, stolen and sold online because of data disclosures. Despite warnings about the severe impact of data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers. App. B5, ¶ 1.

Plaintiffs' Complaint further alleges that cybercrime has been on the rise for the past decade and continues to climb exponentially, with stolen PI often trafficked on the "dark web." App. B31-B32, ¶¶ 73-75. Tech experts have warned that fraudsters harvest drivers' license numbers because they are highly valuable pieces of PI. App. B6, ¶ 3. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200. *Id.* "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, . . . use the information to craft curated social engineering phishing attacks, ... [or use them] to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . .." App. B34-B35, ¶ 82.

[2] App. A1-A16 is the Trial Court's Amended Decision and Order on Motion to Dismiss (Doc. 49), which the Trial Court entered on 6-25-2024, one day after its original Decision and Order on Motion to Dismiss (Doc. 48). The only change in the Amended Decision and Order was the addition of one item in the top left box of the chart on p. 5. Plaintiffs include for convenience of review the Trial Court's original Decision and Order on Motion to Dismiss in the Appendix as App. D1-D16.

Multiple experts have confirmed that drivers' license numbers are particularly useful to identity thieves for applying for unemployment or other government benefits. App. B27, B34-B35, ¶¶ 63, 80-82.

C. American Family decided to send driver's license information out over the internet through their online quoting platforms.

Plaintiffs' Complaint sets forth that the American Family Defendants sell insurance products, including vehicle, home, life, renters', and business insurance, to Americans across the country. App. B6, B16, ¶¶ 4, 39. As part of their insurance sales business, the American Family Defendants operate public facing websites that have an "instant quote" feature available to all persons capable of accessing it via the internet. App. B16-B17, ¶¶ 40-43. Visitors to American Family's insurance websites can "Get A Quote" instantly after providing some limited personal information. *Id.* Despite the many warnings about the severe impact of identity theft on Americans of all economic strata, Defendants put their own economic interest in greasing the wheels to sell more policies ahead of consumers' privacy interests. App. B5, B8-B9, B11-B12, B53, B66, ¶¶ 1, 10-11, 21, 152, 204-205. As Plaintiffs allege, American Family contracted with a third-party "prefill supplier" that "prefills certain information in the online quoting form (such as driver's license number) after a consumer enters personal information into the form." App. B7, B16, ¶¶ 8, 42. Defendants' quoting platforms use the information entered by website visitors, combine it with additional information, including drivers' license numbers, by automatically retrieving matching information from databases and third party prefill suppliers, and use the combined information to provide a quote for insurance. *Id.* To make the quoting process easier for consumers, American Family readily provided consumers' drivers' license numbers to anyone who entered a person's name, address and/or date of birth into their online quoting system. App. B8, ¶¶ 10, 11.

D. The Data Disclosures: Malicious actors accessed consumers' drivers' license numbers on American Family's online quoting websites.

Many data breaches occur when hackers penetrate a company's inadequate security measures and steal consumers' personal information from a company database. Here, however, Plaintiffs allege that the American Family Defendants actually retrieved consumers' private drivers' license information from protected databases and knowingly and negligently sent it over the Internet through their online quoting platforms directly to malicious actors, who were targeting that information in order to commit identity theft. App. B8-B10, B17, B68, B71, ¶¶ 10-15, 43, 211, 221. As alleged in the Complaint, according to its disclosures to the New Hampshire Attorney General, on March 18, 2021, American Family's prefill supplier notified it that Defendants' instant quote feature was being exploited by malicious actors using it to obtain drivers' license numbers and addresses of Plaintiffs and the members of the Class. App. B10-B11 ¶¶ 16-18. Defendants reported that between January 19 and 29, 2021 (for Midvale), and between February 6, 2021 and March 19, 2021 (for AmFam), Defendants "believe unauthorized parties [i.e., malicious actors] may have used an automated bot process to obtain [Plaintiffs'] driver's license number[s] by entering personal information (such as your name and address) they acquired from unknown sources into [Defendants'] quoting platform[s]." App. B9-B10, ¶¶ 15-16 (emphasis added). This means that for an unknown period between at least January 19 and March 19, 2021, Defendants Midvale and AmFam voluntarily made Plaintiffs' and Class Members' drivers' license numbers publicly available on Defendants' online platforms. App. B9-B11, B18, B62-B63, ¶¶ 15-18, 47, 189. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI [drivers' license numbers] without the consent or authorization of the person whose PI was being provided. App. B35, B66, B68, B72, B75, ¶¶ 83, 204, 214, 225, 241.

As Plaintiffs' Complaint sets forth, after Midvale's and AmFam's Data Disclosures, Defendants made amorphous, self-serving statements that they had taken the instant quote platforms offline on March 19, 2021, "blocked the activity," and "enhanced [their] security controls" App. B19-B24, ¶¶ 49-51. In fact, however, American Family engaged in a third, virtually identical Data Disclosure nine months after the first two, except involving online quotes for life insurance rather than automobile insurance (the "Park Data Disclosure"). App. B11, ¶ 21. (Together, all three are the "Data Disclosures.")

E. Defendants promised to keep consumers' private information safe.

Plaintiffs allege that Midvale promises to "protect the confidentiality of the information that we have about you by restricting access to those employees who need to know that information to provide our products and services to you. We maintain physical electronic and procedural safeguards that comply with federal and state regulations to guard your information." App. B6-B7, ¶ 5. Plaintiffs further allege that American Family "recognize[s] the importance of our customers' trust. Keeping personal information confidential is a top priority for all American Family Insurance employees, agents and staff." *Id.* Plaintiffs' Complaint details how Defendants failed to keep these promises; instead, Defendants readily provided Plaintiffs' and putative Class Members' drivers' license numbers to anyone who entered a person's name, address and/or date of birth into their online quoting systems. Thus, customers, prospective customers, and even members of the public who were not prospective customers, had this sensitive personal information made available to the public. App. B8, ¶ 11.

F. Defendants sent "Notices of Data Breach" to Plaintiffs alerting them that "unauthorized parties" (malicious actors) had targeted their drivers' license numbers and warning them "that this data may be used" to file fraudulent unemployment insurance claims in their names.

Plaintiffs' Complaint sets forth that Defendants sent Plaintiffs Baysal, Italiano, and Maxim Notices of Data Breach dated May 13, 2021, and Plaintiff Park a Notice of Data Breach dated January 14, 2022, stating that their PI, including their

drivers' license numbers, was exposed in the Data Disclosures. App. B19-B22, B46-B50, ¶¶ 49, 50, 116, 123, 129, 138. The Notices sent to Plaintiffs and members of the Class informed them that "unauthorized parties may have requested a quote in your name and may have obtained your driver's license number." App. B19-B24, ¶¶ 49-51. The Notices also revealed that Plaintiffs were victims of the Data Disclosures despite a lack of prior relationship with American Family, explicitly noting that Plaintiffs were only affected if they had *not* sought an insurance quote. *Id.* The Notices encouraged affected individuals to use the identity theft protection service American Family offered to "help protect you," and acknowledged the substantial and imminent increased risk of future harm (including identity theft) to Plaintiffs and the Class:

> *We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name*. Please carefully review any written communications you receive from your state's unemployment agency, especially if you have not applied for unemployment benefits. If you suspect that your data has been used to fraudulently apply for unemployment benefits, you should contact the relevant state unemployment agency immediately.

Id. (emphasis added).

G. American Family's Data Disclosures Injured the Plaintiffs and the Class.

Plaintiffs' Complaint alleges that the PI at issue in the Data Disclosures, which includes at least drivers' license numbers, is significantly more valuable than the loss of, for example, credit card information in a retail data breach. There, victims can cancel or close credit and debit card accounts. Drivers' license numbers are difficult and highly problematic to change. App. B33, ¶ 78. In fact, drivers' license numbers are known targets for attacks like the Data Disclosures, because they are a "critical part of a fraudulent, synthetic identity." App. B6, ¶ 3. Drivers' license numbers are "connected to . . . vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment . . . , doctor's offices, government agencies, and other entities." App. B34, ¶ 81. In fact, "[h]aving access to that one number can provide an identity thief

with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves." *Id.* (emphasis added). Plaintiffs' Complaint alleges that each of the four named Plaintiffs was harmed by American Family's failure to secure their PI. App. B9-B10, B25, B27, B45, B52, B54-B56, B77, B79, ¶¶ 25, 54-55, 62, 114, 145, 156-161, 247, 256. Plaintiffs Baysal, Maxim, Italiano, and Park never sought a quote for insurance of any kind from American Family. App. B13-B14, ¶¶ 27-30. Despite never authorizing American Family to have, use, or otherwise possess their drivers' license numbers, each received a Notice indicating that their drivers' license numbers were subject to a Data Disclosure. App. B13-B14, B19-B24, ¶¶ 27-30, 49-54. Plaintiffs' Complaint further alleges that each Plaintiff spent time responding to the Data Disclosures and continues to work to keep their PI secure. App. B46-B51, ¶¶ 118-119, 124-125, 133-134, 139-141. Furthermore, both Plaintiff Baysal and Plaintiff Maxim were subject to unemployment benefits fraud in New York following the Data Disclosures. App. B46-B47, B49, ¶¶ 117-118, 130. In other words, two of the named Plaintiffs in this case experienced the exact type of identity theft that American Family predicted when they wrote in their Notices of Data Breach: "We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name." App. B46-B48, B50, ¶¶ 116, 123, 129, 138.

In addition, both Plaintiff Maxim and Plaintiff Park were subject to a flurry of fraudulent financial accounts and charges in their names in the wake of the Data Disclosures. Plaintiff Maxim received a letter from Charles Schwab indicating that a fraudulent brokerage account had been opened in his name, and when he checked his credit report in August 2021, he discovered a soft inquiry from Klarna that involved an unauthorized purchase from Foot Locker. App. B49, ¶¶ 131-133. He also discovered that a fraudulent new phone number had been added to his credit report. *Id.* Plaintiff Park received notice from Wells Fargo Bank dated January 6, 2022, stating someone had completed an online application and unsuccessfully attempted to open an account in his name—likely someone utilizing his PI obtained

as part of the Data Disclosure. App. B50-B51, ¶¶ 139-140. Plaintiff Park spent time calling Wells Fargo Bank to report the fraudulent attempt to open an account in his name. *Id.* He spent additional time and effort filing a police report about the incident. *Id.* Plaintiff Park then received a letter from JPMorgan Chase Bank, N.A., dated January 17, 2022, stating someone had unsuccessfully applied for a CHASE SAPPHIRE Visa Signature account in his name—again, likely someone utilizing his PI obtained as part of the Data Disclosure. *Id.* Plaintiff Park spent time calling Chase Bank to report the fraudulent attempt to open an account in his name. *Id.* He spent additional time and effort filing a police report about the incident. *Id.* Prior to these two incidents that occurred within two months of the Data Disclosure, Plaintiff Park had never been a victim of attempted identity theft and fraud. *Id.*

In an effort to head off any fraudulent applications for unemployment insurance in her name and at the direction of the notice Defendants provided, Plaintiff Italiano contacted the Florida Reemployment Assistance Program to place a fraud alert notifying them that she was a victim of the Midvale Data Disclosure. App. B47-B48, ¶ 124.

STANDARD OF REVIEW

"Whether a party has standing is a question of law" that the Court of Appeals reviews "independently." *Friends of Black River Forest v. Kohler Co.*, 2022 WI 52, ¶10, 402 Wis. 2d 587, 977 N.W.2d 342 (Wis. 2022) (citation omitted). Under Wisconsin law, the standing of a party whose interest is challenged is determined by (1) personal interest in the controversy; (2) injury or adverse effect; and (3) judicial policy that "calls for protecting the interest of the party whose standing has been challenged." *Foley-Ciccantelli v. Bishop's Grove Condo Ass'n, Inc.*, 2011 WI 36, ¶5, 333 Wis. 2d 402, 797 N.W.2d 789. The law of standing is liberally construed. *Krier v. Vilione*, 2009 WI 45, ¶20, 317 Wis. 2d 288, 766 N.W.2d 517 (Wis. 2009).

ARGUMENT

I. The Trial Court Erred by Finding that Plaintiffs Lacked Standing to Bring this Case in the Wisconsin State Courts.

A. The Trial Court Erred by Failing to Apply this Court's Binding Precedent on Standing in the Data Breach Context – *Reetz v. Advocate Aurora Health, Inc.* – to Find Plaintiffs Have Standing.

"'Standing' is a concept that restricts access to judicial remedy [and so] the law of standing should be liberally construed." *Krier v. Vilione*, 2009 WI 45, ¶ 20, 317 Wis. 2d 288, 766 N.W.2d 517, 524; *see also Reetz v. Advocate Aurora Health, Inc.*, 2022 WI App 59, ¶ 7, 405 Wis. 2d 298, 310, 983 N.W.2d 669, 676 (Wis. Ct. App. 2022) ("*Reetz*") (citing *Krier* in the data breach context: "The law of standing is liberally construed.") "Under Wisconsin law, the standing of a party whose interest is challenged is determined by: (1) personal interest in the controversy; (2) injury or adverse effect; and (3) judicial policy that 'calls for protecting the interest of the party whose standing has been challenged.'" *Reetz*, 2022 WI App 59 at ¶7, 405 Wis. 2d 298 at 310, 983 N.W.2d 669 at 675-6 (quoting *Foley-Ciccantelli v. Bishop's Grove Condominium Ass'n, Inc.*, 2011 WI 36 ¶ 5, 333 Wis. 2d 402, 797 N.W.2d 517 (Wis. 2011)).

The case law surrounding "standing" in Wisconsin state courts has encompassed "various tests that have been applied in administrative review cases, in constitutional law cases, and in declaratory judgment cases. These various tests, while at times inconsistently used by courts, when appropriately used *in particular types of cases* are tools for determining *personal interest, adverse effect, and judicial policy,* the three essential aspects of standing." *Foley-Ciccantelli v. Bishop's Grove Condominium Ass'n, Inc.*, 2011 WI 36 ¶ 6, 333 Wis. 2d 499, 424 N.W.2d 789, 793(Wis. 2011) (emphasis added). Thus, the Wisconsin Supreme Court has made clear that the application of the general principles of "standing" within state court cases will vary depending on the "particular type of case[]." *Id.*

In *Reetz*, this Court (the Court of Appeals of Wisconsin) examined "standing" in the context of a data breach case and provided the "tools for determining"

standing in this "particular type[] of case." *Reetz*, 2022 WI App 59, ¶¶ 7-10, 405 Wis. 2d 298, 310-313, 983 N.W.2d 669, 675-676. As the only higher court ruling applying Wisconsin state standing principles in a data breach case, this Court's ruling in *Reetz* is binding on the Trial Court, and yet the Trial Court failed even to mention it. App. A1-A16; *Community Dev. Auth. v. Racine County Condemnation Comm'n*, 2006 WI App 51, ¶ 21, 289 Wis. 2d 613, 712 N.W.2d 380; *see also* Wis. Stat. § 752.41(2) ("Officially published opinions of the court of appeals *shall have statewide precedential effect.*") (emphasis added).

In *Reetz*, this Court held that: "To establish standing in a data breach identity theft case, allegations of time spent dealing with fraud attempts, the threat of future identity theft, and money spent mitigating that threat *are sufficient to establish standing*." *Reetz*, 2022 WI App 59 at ¶ 8, 405 Wis. 2d 298 at 311, 983 N.W.2d 669 at 676 (cleaned up) (emphasis added). Plaintiffs here *have* alleged "time spent dealing with fraud attempts [and actual fraud], the threat of future identity theft [again, based on instances of actual fraud], and money spent mitigating that threat." *Id.*

Under *Reetz*, any one of those allegations would be "sufficient to establish standing" in the data breach context. For example, when the defendant in *Reetz* challenged whether *reimbursed* overdraft fees would constitute "actual damages," the Court held: "Further, [Plaintiff's] damages do not arise only from the overdraft fees, but from allegations of time spent dealing with fraud attempts [and] the threat of future identity theft." *Id.* at ¶ 13, 983 N.W.2d at 677-678. In other words, where identity fraud has occurred, time spent dealing with it and the threat of additional future identity theft constitute "injury" or "adverse effect," even where the fraud does not ultimately come out of the plaintiff's pocket. *Id.*

Plaintiffs allege "time spent dealing with fraud attempts, the threat of future identity theft, and money spent mitigating that threat." Shortly following the Data Disclosures, Plaintiffs were victims of *actual fraud attempts using their PI*. In fact, both Plaintiff Baysal and Plaintiff Maxim were subject to the *exact type of fraud*

American Family predicted in its Notices of Data Breach: *fraudulent applications for unemployment benefits made in their names*. App. B46, B49, ¶ 117 (Baysal); ¶¶ 130-132 (Maxim). In addition, Plaintiff Maxim and Plaintiff Park experienced a flurry of fraudulent accounts opened in their names. App. B49-B51, ¶¶ 130-132 (Schwab and Klarna/Footlocker accounts – Maxim); ¶¶ 139-140 (Wells Fargo and JP Morgan Chase;/Chase Sapphire accounts – Park). Despite this *actual fraud conducted against these named plaintiffs*, the Trial Court wrongly denied that the Plaintiffs have "standing to pursue the current action." App. A12. In doing so, the Trial Court never once even mentioned this Court's *Reetz* decision, which clearly states that time spent dealing with fraud attempts, the threat of future identity theft, and money spent mitigating that threat confers standing in a data breach case. Instead, the Trial Court only quoted from the prior federal case orders that analyzed standing in the context of Article III jurisdictional standing under the U.S. Constitution. App. A10. Plaintiffs will explain in the following section why Article III jurisdictional standing has no application in state court. Plaintiffs explain here, however, how the Trial Court erred when it ignored this Court's binding precedent in *Reetz*; did not apply it; and did not, in fact, even mention it. *Reetz* is the law the state Trial Court was bound to follow, and its failure to recognize that is fatal.

1. The Trial Court erred by denying that the unemployment fraud American Family predicted, and Plaintiffs experienced, was harm to the Plaintiffs and was plausibly tied to the Data Disclosures.

It is important to deal first with the unemployment fraud committed in Plaintiffs' names. American Family's Notices of Data Breach acknowledged the causal connection between the Data Disclosures and this type of identity fraud, which then did happen to Plaintiffs Baysal and Maxim. In light of these facts, it is astonishing that Defendants and the Trial Court claim that Plaintiffs have not alleged injury-in-fact. *They suffered the exact identity theft American Family* warned was a foreseeable result of the Data Disclosure, and which the NYDFS *identified as the*

goal of the malicious actors who received Plaintiffs' drivers' license numbers from Defendant insurers. App. B39-40, B46, B49, B63, B67, ¶¶ 97, 99, 117, 130, 191, n. 61, n. 62, 208. Under these facts, it is frankly impossible to deny that the unemployment fraud using Plaintiffs' names is plausibly connected to these Data Disclosures. However, instead of leading with this actual fraud that also gives rise to other related damages such as time spent addressing it and increased risk of future identity theft, the Trial Court buried this fact towards the end of its analysis of Plaintiffs' injuries – on page 15 of 16 in its Order. App. A15-A16. If Plaintiffs have alleged actual fraud effected with use of their disclosed drivers' license numbers, then, under *Reetz*, they are entitled to claim at least (1) lost time dealing with fraud attempts, (2) the threat of future identity theft, and/or (3) money spent mitigating that threat. The Trial Court avoided this logic by dismissing the Plaintiffs' right to time, expenses incurred, and the threat of future additional fraud first, on pages 13-14, and only then making a cursory review of the unemployment fraud Plaintiffs actually experienced on page 15. App. A13-A15. And in this belated review, the Trial Court first erred by denying the obviously reasonable inference that the very unemployment fraud American Family and the NYDFS predicted would happen due to the Data Disclosures was in fact related to the Data Disclosures. ("This claim fails to connect disclosure of their drivers' license in this data breach to any fraudulent application for unemployment benefits." App. A15.)

The Trial Court also erred by denying the injury caused to an individual when a fraudulent application for benefits is filed *in that individual's name*. The Trial Court cavalierly cited one unpublished North Carolina non-data breach case to argue that unemployment fraud is only "harm to the state." *Id.* The case is entirely inapposite because the plaintiff there was *not* the subject of the fraudulent application and was *not* claiming identity theft of any kind, but was generally complaining that someone against whom he had a grudge had committed unemployment fraud against North Carolina. *Campbell v. Gaither*, No. 3311-cv-190-FDW, 2011 WL 1838779, at *3 (W.D.N.C. May 13, 2011). Here, the fraudulent

applications *were made in these Plaintiffs' names* –compromising their own access to their state accounts, subjecting them to potential criminal liability, and unquestionably requiring them to spend substantial time clearing up this fraud. And even if the states ultimately determine that Plaintiffs will not be held responsible for these fraudulent claims in their names, they still cause money damages in the time spent to clear them up, just as with the overdraft fees in *Reetz*: "Money damages may arise from a data breach because. . . the value of one's own time needed to set things straight is a loss from an opportunity cost perspective." *Reetz*, 2022 WI App. 59, ¶ 12, 983 N.W.2d at 677. The law is clear, as are the facts here. The Trial Court's cavalier dismissal of this injury, failure to consider all reasonable inferences in Plaintiffs' favor, and failure to apply the law as set forth in R*eetz*, constitute error requiring reversal.

2. The Trial Court also erred by denying that the fraudulent financial accounts opened in Plaintiffs' names were harm to the Plaintiffs and were plausibly tied to the Data Disclosures.

Similarly, the Trial Court erred when it denied Plaintiffs had alleged actual damages based on fraudulent financial accounts opened and charges made in their names in the wake of the Data Disclosures. App. A15-A16. The Trial Court first made the same mistake it did with regard to the unemployment fraud by denying the harm caused by such fraud: "They also do not allege how they were harmed by this;" and "Furthermore, the transaction was unsuccessful." *Id.* Again, where financial fraud is attempted, "Money damages may arise from. . . the value of one's own time needed to set things straight. . . ." *Reetz*, 2022 WI App. 59, ¶ 12, 983 N.W.2d at 677. The Trial Court also erred by making complex findings of fact denying causation at this stage of the case: "[Plaintiffs] have not demonstrated that these [fraudulent account] incidents were a consequence of the disclosure of their driver's license numbers." App. A15. In other words, the Trial Court required Plaintiffs to demonstrate proximate cause. But "proximate cause is "fact laden and inappropriate for a motion to dismiss at the pleadings stage." *GEICO*, 2023 WL

5524105, at *5. "The question of whether the injury alleged will result from the [defendant's] action in fact is a question to be determined on the merits, not on a motion to dismiss for lack of standing." *Friends of Blue Mound v. Dept. of Nat. Res.*, 2023 WI App 38, ¶ 26, 408 Wis. 2d 763, 993 N.W.2d 788, 798-799 (Wis. App. 2023) (quoting *Wisconsin's Env't Decade, Inc. v. Pub. Serv. Comm'n of Wis.* (*WED I*), 69 Wis. 2d 1, 14, 230 N.W.2d 243 (Wis. 1975)). And where, as here, Plaintiffs have alleged "that hackers cross-referenced the data from the breaches and combined it with data from other sources to create 'fullz packages,'" the question whether that combined information led to the flurry of fraudulent accounts Plaintiffs experienced following the Data Disclosures is "an issue of causation that will need to be resolved at trial or summary judgment. At this stage plaintiffs have alleged injuries that are fairly traceable to" the Data Disclosures. *Fox v. Iowa Health System*, 399 F. Supp. 3d 780, 792 (W.D. Wis. 2019). Just as in *Fox*, Plaintiffs here alleged at length how fraudulent financial accounts can be connected to the taking of drivers' license numbers, especially where the malicious actors were building "fullz" profiles on them and used Defendants' websites to obtain the additional credential of the driver's license number. App. B28, B34, B36-B37, ¶¶ 65, n. 25, 80, 86, 89.

The Trial Court erred by ignoring this Court's controlling test set forth in *Reetz* to apply Wisconsin standing principles in this "particular type of case" and denying Plaintiffs "access to judicial remedy" by ruling that they lack standing.

B. The Trial Court Erred by Recycling the Federal Courts' Article III Jurisdictional Standing Analysis Which Does Not Apply in State Court and Certainly Does Not Overturn Reetz.

Plaintiffs openly acknowledge that this case has previously proceeded before the federal courts (U.S. District Court for the Western District of Wisconsin and the U.S. Court of Appeals for the Seventh Circuit), which held that they did not have jurisdiction to consider the case for lack of Article III standing. *Baysal v. Midvale Indemnity Company*, 2022 WL 1155295 (W.D. Wis. April 19, 2022) (*Baysal I*);

Park v. American Family Life Ins. Co., 608 F. Supp. 3d 755 (W.D. Wis. 2022); *Baysal v. Midvale Indemnity Company*, 78 F.4th 976 (2023) (*Baysal II*). Because Article III of the U.S. Constitution is a jurisdictional provision that does not apply to state courts, the Trial Court erred in effectively copying those decisions rather than following this Court's controlling precedent in *Reetz*.

Article III standing derives from the provision of the U.S. Constitution that limits federal courts to "cases" and "controversies," as defined by the U.S. Supreme Court and other federal courts, because, unlike state courts, federal courts are courts of limited jurisdiction. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203, 2207 (2021). A determination by a federal court that Article III standing is lacking is a determination that it has no jurisdiction to hear the case. *See, e.g.*, *Davis v. Federal Election Commission*, 554 U.S. 724, 732–33, 128 S. Ct. 2759, 171 L.Ed.2d 737 (2008); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559–60, 112 S. Ct. 2130, 119 L.Ed.2d 351 (1992). By definition then, the federal court has no jurisdiction to address the merits of the claims and all dismissals for lack of Article III standing are without prejudice. *See, e.g., Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 94–95, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998). Thus, Plaintiffs did not receive a hearing on the merits of their case in the federal courts, and their case was dismissed without prejudice.

By contrast: "[S]tate courts are courts of general jurisdiction—essentially open to all comers on all matters. . . ." *East Central Illinois Pipe Trades Health & Welfare Fund v. Prather Plumbing & Heating, Inc.*, 3 F.4th 954, 957 (7th Cir. 2021); *see also Nike, Inc. v. Kasky*, 539 U.S. 654, 661-62 & n.2, 123 S.Ct. 2554 (2003) (Stevens, J., concurring) (emphasizing that, although federal courts could not exercise jurisdiction because the respondent lacked Article III standing, those "constraints . . . do not apply in state courts," which remain "free to adjudicate th[e] case"). "Permitting state courts to entertain federal causes of action facilitates the enforcement of federal rights. If Congress does not confer jurisdiction on federal courts to hear a particular federal claim, the state courts stand ready to vindicate the

federal right. . .” *Gulf Offshore Co. v. Mobil Oil Corp.*, 453 U.S. 473, 478 n.4, 101 S. Ct. 2870, 2875, 69 L. Ed. 2d 784 (1981) (citing *Martin v. Hunter's Lessee*, 1 Wheat. 304, 346–48, 4 L.Ed. 97 (1816)). Thus, the Trial Court’s wholesale adoption of the federal court’s Article III standing analysis mistook the broad powers inherent in the state court for the jurisdictionally limited powers of the federal courts.

1. The federal cases were poorly decided and created a conflict with other federal courts hearing essentially identical cases against other insurers who committed similar data disclosures.

Plaintiffs thoroughly disagree with the federal courts’ rulings denying Article III standing in the related federal cases. One judge on the Seventh Circuit panel wrote a vigorous, well-reasoned (and frankly correct) dissent. *Baysal II*, 78 F.4th at 980-990. By denying Article III standing in this case, the Seventh Circuit conflicted with multiple U.S. District Courts that are proceeding with or have concluded litigation on essentially the same case against GEICO, Travelers, USAA, and Farmers. *See, e.g.*, *In re GEICO Customer Data Breach Litig.*, No. 21-CV-2210-KAM-SJB, 2023 WL 4778646, at *9 (E.D.N.Y. July 21, 2023), *report and recommendation adopted*, 2023 WL 5524105 (E.D.N.Y. Aug. 28, 2023) (where “Plaintiffs spent significant time, effort, and resources addressing the allegedly fraudulent bank accounts, credit card charges, and unemployment claims taken out in their names,” they had Article III standing to proceed against GEICO); *Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55, 66, 68 (S.D.N.Y. 2022) (“Here, plaintiff adequately pleads injuries-in-fact in the form of a loss of privacy, as well as the harm incurred by attempting to mitigate existing and future identity theft,” and an “objectively reasonable likelihood that an injury will result” from automatic disclosure of drivers’ license numbers in online quotes); *In re USAA Data Security Litig.*, 621 F. Supp. 3d 454, 473 (S.D.N.Y. Aug. 12, 2022) (“Because plaintiffs plausibly allege the continued inadequacy of USAA's security measures, they plausibly allege that they face a substantial risk of future harm if USAA's security shortcomings are not redressed”); *Stallone v. Farmers Group, Inc.*, No.

221CV01659GMNVCF, 2022 WL 10091489, at *10 (D. Nev. Oct. 15, 2022) ("the Court is persuaded that Plaintiff has sufficiently alleged a concrete injury was suffered due to the failed Eddie Bauer credit application. . . . Information was stolen, has already surfaced on the Internet, and been misused by others. Given this, the danger that Plaintiffs' data will be subject to further misuse can be described as 'certainly impending.'").

Plaintiffs firmly believe they and the class of individuals exposed by American Family deserve the same redress as the plaintiffs exposed by GEICO, USAA, Travelers, and Farmers. The fact that the American Family Defendants in this case have permitted three successive Data Disclosures by the same mechanism on their instant quote websites is particularly egregious and calls even more for their being held accountable. After the Seventh Circuit predictably denied Plaintiffs' request for *en banc* review,[3] Plaintiffs were faced with the choice of petitioning the U.S. Supreme Court for certiorari, or re-filing the case in state court, where Article III does not apply:

> The Court does not prohibit Congress from creating statutory rights for consumers; it simply holds that federal courts lack jurisdiction to hear some of these cases. That combination may leave state courts—which ''are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law,'' *ASARCO Inc. v. Kadish*, 490 U.S. 605, 617, 109 S.Ct. 2037, 104 L.Ed.2d 696 (1989)—as the sole forum for such cases, with defendants unable to seek removal to federal court. See also Bennett, The Paradox of Exclusive State-Court Jurisdiction Over Federal Claims, 105 Minn. L. Rev. 1211 (2021). By declaring that federal courts lack jurisdiction, the Court has thus ensured that state courts will exercise exclusive jurisdiction over these sorts of class actions.

[3] "Rehearing *en banc* is rare in the U.S. Court of Appeals for the Seventh Circuit. [There is] as great a chance of persuading the U.S. Supreme Court to grant certiorari as . . to persuade the Seventh Circuit to grant rehearing *en banc*." https://www.jenner.com/a/web/2mkDqvvmn9MhNGuK9txJ3X/4HRMZQ/Brody%2520law.com%25209%252025%252019.pdf?1569950150#:~:text=Rehearing%20en%20banc%20is%20rare,a%20new%20rule%20or%20procedure.)

TransUnion, 141 S. Ct. 2190 at 2224, n. 9 (Thomas, dissenting). In accord with Justice Thomas's advice, Plaintiffs chose filing in state court as the best option for seeking redress for the class of individuals exposed by the American Family Defendants to the "systematic and aggressive campaign" of malicious actors leveraging insurers' instant quote platforms to access drivers' license numbers for use in fraudulent unemployment claims and other identity theft.

2. By following the federal cases instead of Reetz, the Trial Court misunderstood the nature of Wisconsin's "standing" principles for state court cases.

If Article III standing does not apply to Wisconsin state court cases, why did American Family, and at its behest, the Trial Court, reflexively argue that the state court should follow the federal courts and refuse to consider the merits of Plaintiffs' claims on the basis of "standing?" They suffer from a misconception of the "standing" principles that do apply in Wisconsin state courts. Upon examination, the cases cited in the court below explicitly recognize that: "our state constitution *lacks the jurisdiction-limiting language of its federal counterpart* [i.e., Article III, and so] 'standing in Wisconsin *is not a matter of jurisdiction. . . .*'" *Friends of Black River Forest v. Kohler Co.*, 2022 WI at 52 ¶17 (Wis 2022). (emphasis added). Rather, Wisconsin courts evaluate standing principles only in terms of "sound judicial policy." *Id.* Ultimately, this boils down to a question "whether the party's asserted injury is to an interest protected by a statutory or constitutional provision." *Foley-Ciccantelli v. Bishop's Grove Condominium Ass'n, Inc.*, 2011 WI 36 ¶ 55, 333 Wis. 2d 499, 505, 424 N.W.2d 789 (lead opinion) (Wis. 2011).

The sparse Wisconsin cases that the Trial Court mentions to justify dismissing this case on prudential standing principles do not include data breach cases and certainly do not overrule *Reetz*, which does address "standing" in the context of a data breach case and is binding on the Trial Court. *See, e.g., Alsteen v. Wauleco, Inc.*, 2011 WI App. 105, ¶¶ 9-11, 333 Wis. 2d 473, 479-480, 802 N.W.2d 212, 215 (Wis. Ct. App. 2011) (plaintiff's allegations related to medical monitoring

in toxic tort case, and the court found that an increased risk of cancer is not an actual injury); *Howard v. Mt. Sinai Hosp., Inc.*, 63 Wis. 2d 515, 520-21, 217 N.W.2d 383, 386, (Wis. 1974)(in medical malpractice case where negligence is conceded due to four pieces of a catheter left inside patient, fear or phobia of cancer was too remote to be an element of the damages); *Meracle v. Children's Serv. Soc. of Wis.*, 149 Wis. 2d 19, 437 N.W.2d 532, 533, 535 (Wis. 1989) (adoptive parents' claim for adoption agency's negligent misrepresentation of adoptee's likelihood of developing Huntington's disease did not accrue until adoptee developed Huntington's disease). None of these cases justifies the Trial Court's failure to follow this Court's binding precedent in *Reetz*. The Trial Court erred in adopting the inapplicable federal Article III analysis from the prior *Baysal* cases rather than following this Court's holdings for how to apply Wisconsin's prudential standing principles in the data breach context, as set forth in *Reetz*. Furthermore, because standing is not jurisdictional in state court, the fact that Plaintiffs have pleaded injury and damages in the data breach context sufficient to support standing also means that same injury and damages state a claim. *Reetz*, 983 N.W.2d at 679 ("Reetz has successfully stated a claim for negligence and pleaded damages in support of her claim.")

CONCLUSION

Plaintiffs respectfully request that this Court reverse the Trial Court's order granting the American Family Defendants' motion to dismiss and remand to the Trial Court for further proceedings consistent with this Court's decision.

Respectfully submitted this 14th day of October 2024,

Dated: October 14, 2024

/s/ Electronically Signed by Jessica N. Servais
Jessica N. Servais (WI # 1048014)
Kate M. Baxter-Kauf (admitted *pro hac vice*)
Karen Hanson Riebel (admitted *pro hac vice*)
Maureen Kane Berg (admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
jnservais@locklaw.com
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

Gayle M. Blatt
P. Camille Guerra
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com
camille@cglaw.com

Attorneys for Plaintiffs-Appellants

CERTIFICATION BY ATTORNEY

I certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 7,243 words.

I further certify that filed with this brief is an appendix that complies with Wis. Stat. § 809.19 (2)(a) and that contains, at a minimum: (1) a table of contents; (2) the findings or opinion of the circuit court; (3) a copy of any unpublished opinion cited under Wis. Stat. § 809.23 (3) (a) or (b); and (4) portions of the record essential to an understanding of the issues raised, including oral or written rulings or decisions showing the circuit court's reasoning regarding those issues.

I further certify that if this appeal is taken from a circuit court order or judgment entered in a judicial review of an administrative decision, the appendix contains the findings of fact and conclusions of law, if any, and final decision of the administrative agency.

I further certify that if the record is required by law to be confidential, the portions of the record included in the appendix are reproduced using one or more initials or other appropriate pseudonym or designation instead of full names of persons, specifically including juveniles and parents of juveniles, with a notation that the portions of the record have been so reproduced to preserve confidentiality and with appropriate references to the record.

I further certify that I have submitted an electronic copy of this brief which complies with the requirements of Wis. Stat. § 809.19(12). I further certify that this electronic brief is identical in content and format to the printed form of the brief filed as of this date. A copy of this certificate has been served with and paper copies of this brief filed with the court and served on opposing parties.

Dated: October 14, 2024

/s/ Electronically Signed by Jessica N. Servais

Jessica N. Servais (WI # 1048014))
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South

Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
jnservais@locklaw.com

Attorney for Plaintiffs-Appellants