In the

United States Court of Appeals

For the Seventh Circuit

No. 14-3700

JOHN LEWERT, on behalf of himself and all others similarly situated, *et al.*,

Plaintiffs-Appellants,

v.

P.F. CHANG'S CHINA BISTRO, INC.,

Defendant-Appellee.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
Nos. 14 C 4787, 14 C 4923 — **John W. Darrah**, *Judge*.

ARGUED JANUARY 13, 2016 — DECIDED APRIL 14, 2016

Before WOOD, *Chief Judge*, and BAUER and HAMILTON, *Circuit Judges*.

WOOD, *Chief Judge*. About two months after they dined at P.F. Chang's China Bistro, in Northbrook, Illinois, John Lewert and Lucas Kosner received the unwelcome news that the restaurant's computer system had been hacked and debit- and credit–card data had been stolen. Lewert and Kosner brought separate suits, which were later consolidated, seek-

ing damages resulting from the theft on behalf of themselves and a class. Concluding that they had not suffered the requisite personal injury, the district court dismissed for lack of standing. FED. R. CIV. P. 12(b)(1). In light of *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015), we reverse and remand for further proceedings.

I

P.F. Chang's operates a chain of restaurants throughout the United States. On June 12, 2014, the company announced that its computer system had been breached and some consumer credit- and debit–card data had been stolen. At the time, it did not know how many consumers were affected, whether the breach was general or limited to specific locations, or how long the breach lasted. As a precaution, it switched to a manual card–processing system at all locations in the continental United States and encouraged its customers to monitor their card statements. News articles indicated that the breach might have begun as far back as September 2013. Later that summer, on August 4, 2014, P.F. Chang's announced that it had determined that data was stolen from just 33 restaurants. The only affected restaurant in Illinois, it reported, was at the Woodfield Mall in Schaumburg (a suburb of Chicago).

Kosner dined at a different P.F. Chang's, located in Northbrook, on April 21, 2014, and paid with his debit card. On June 8, 2014, four fraudulent transactions were made with the card he had used, and so he cancelled it immediately. Later in June, Kosner learned about the breach at P.F. Chang's. Putting two and two together, he noted that the fraudulent charges on his card had appeared shortly after he dined at P.F. Chang's, and he drew the conclusion that his

debit-card data were among those compromised by the breach. Based on that concern, he purchased a credit monitoring service to protect against identity theft, including against criminals using the stolen card's data to open new credit or debit cards in his name. He spent $106.89 on the service.

On April 3, 2014, Lewert dined at the same P.F. Chang's in Northbrook as Kosner later patronized. Lewert, too, paid with his debit card. The consequences for Lewert were less troubling: he did not spot any fraudulent charges on his card, nor did he cancel his card and suffer the associated inconvenience or costs. Lewert did allege, however, that after P.F. Chang's initially announced the breach in June 2014, he spent time and effort monitoring his card statements and his credit report to ensure that no fraudulent charges had been made on that card and that no fraudulent accounts had been opened in his name.

Lewert and Kosner seek to represent a class of all similarly situated customers whose payment data may have been compromised. Their actions were consolidated on June 24, 2014. In the aggregate, the claims they assert on behalf of the class exceed $5,000,000 in value. Minimal diversity exists: Lewert and Kosner are citizens of Illinois, while P.F. Chang's is a Delaware corporation with its principal place of business in Arizona. Putting to one side the central issue of Article III standing, to which we return, the district court therefore had jurisdiction under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2). As we said, the district court dismissed the consolidated action for lack of standing.

II

We consider *de novo* the question whether a plaintiff satisfies the standing criteria imposed by Article III of the Constitution. *Reid L. v. Ill. State Bd. of Educ.*, 358 F.3d 511, 515 (7th Cir. 2004). The district court "must accept as true all material allegations of the complaint, drawing all reasonable inferences therefrom in the plaintiff's favor, unless standing is challenged as a factual matter." *Id.* The plaintiffs, as the "part[ies] invoking federal jurisdiction," bear the burden of establishing Article III standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). They must demonstrate that they have "suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2661 (2013) (citing *Lujan*, 504 U.S. at 560–61).

A

This is not our first time to examine standing in a case involving a data breach. In *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015), the high–end department store Neiman Marcus experienced a data breach that potentially exposed the payment–card data of all customers who paid with cards during the previous year. *Id.* at 690. The store alerted all potentially affected customers and offered a credit monitoring service to each of them. *Id.* The plaintiffs had shopped at Neiman Marcus during the time the information was exposed to the invader. *Id.* They brought a class action based on the breach. *Id.* at 691.

We concluded that several of those plaintiffs' injuries were concrete and particularized enough to support Article III standing. First, we identified two future injuries that were sufficiently imminent: the increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft. *Id.* at 691–94. These, we found, were not mere "allegations of possible future injury," but instead were the type of "certainly impending" future harm that the Supreme Court requires to establish standing. *Id.* at 692 (internal quotation marks omitted) (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013)). In *Clapper*, the plaintiffs expressed only their fear that the government *might* have intercepted their private communications. *Clapper*, 133 S. Ct. at 1148. The Supreme Court held that this injury was too speculative to support standing to challenge the Foreign Intelligence Surveillance Act. *Id.* In contrast, the alleged data theft in *Remijas* had *already* occurred. *Remijas*, 794 F.3d at 693. In the latter situation, we held, "there is 'no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken.'" *Id.* (alteration in original) (quoting *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)). The plaintiffs "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 injury will occur." *Id.* (quoting *Clapper*, 133 S. Ct. at 1147).

Remijas also found injuries sufficient for standing in the time and money the class members predictably spent resolving fraudulent charges (even if the bank ultimately repaid those charges), as well as in the identity theft that had already occurred and in the time and money customers spent

protecting against future identity theft or fraudulent charges. *Id.* at 694. While mitigation expenses qualify as "actual injuries" only when the harm is imminent, the data breach in *Remijas* had already occurred. This made the risk of identity theft and fraudulent charges sufficiently immediate to justify mitigation efforts. *Id.* (citing *Clapper*, 133 S. Ct. at 1152).

In the present case, several of Lewert and Kosner's alleged injuries fit within the categories we delineated in *Remijas*. They describe the same kind of future injuries as the *Remijas* plaintiffs did: the increased risk of fraudulent charges and identity theft they face because their data has already been stolen. These alleged injuries are concrete enough to support a lawsuit. P.F. Chang's acknowledges that it experienced a data breach in June of 2014. It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is "sooner or later[] to make fraudulent charges or assume those consumers' identities[.]" *Id.* at 693. Lewert is at risk for both fraudulent charges and identity theft. Kosner has already cancelled his debit card, but he is still at risk of identity theft. Other members of the would–be class will be in the same position as one or the other named plaintiff.

Similarly, Lewert and Kosner have alleged sufficient facts to support standing based on their present injuries. Kosner asserts that he already has experienced fraudulent charges. Even if those fraudulent charges did not result in injury to his wallet (he stated that his bank stopped the charges before they went through), he has spent time and effort resolving them. He also took measures to mitigate his risk by purchasing credit monitoring for $106.89. Lewert alleged that he has

spent time and effort monitoring both his card statements and his other financial information as a guard against fraudulent charges and identity theft.

P.F. Chang's accepts *Remijas*'s holding that the time and money spent resolving fraudulent charges are cognizable injuries for Article III standing. (We emphasize that we speak only of allegations—whether any compensable losses occurred is a question for the merits.) But it does argue that the plaintiffs' mitigation here was unreasonable because, unlike the situation in *Remijas* and similar data breaches, this one posed a risk only of fraudulent charges to affected cards, not of identity theft. But this is a factual assumption that has yet to be tested. We recognized in *Remijas* that the information stolen from payment cards can be used to open new cards in the consumer's name. *Id.* at 692–93. P.F. Chang's itself implicitly acknowledged this—in its August press release, P.F. Chang's encouraged consumers to monitor their credit *reports* (in part for new-account activity) rather than simply the statements for existing affected cards. This is consistent with *Anderson v. Hannahford Bros. Co.*, in which the First Circuit held that the expenses for replacing cards and purchasing a credit monitoring service were reasonable mitigation after a data breach. 659 F.3d 151, 162 (1st Cir. 2011) (pre-*Clapper*). If P.F. Chang's wishes to present evidence that this data breach is unlike prior breaches and that the plaintiffs should have known this, it is free to do so, but this goes to the merits. As a matter of pleading, nothing suggests that the plaintiffs' mitigation efforts were unreasonable.

P.F. Chang's tries to distinguish this case from *Remijas* by noting that, unlike Neiman Marcus, it contests whether the

plaintiffs' data was exposed in the breach. To the extent this is a valid distinction (and that is questionable), it is one that is immaterial. At the pleading stage, the plaintiffs' factual allegations must "[]cross the line from conceivable to plausible." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Once they have crossed this threshold, we accept them for purposes of a motion to dismiss as true. *Reid L.*, 358 F.3d at 515. The same is true of allegations of standing. *Lujan*, 504 U.S. at 561 (each element of standing "must be supported … with the manner and degree of evidence required at the successive stages of the litigation").

The plaintiffs plausibly allege that their data was stolen. In its June statement, P.F. Chang's addressed customers who had dined at *all* of its stores in the United States and admitted that it did not know how many stores were affected. It is easy to infer that it considered the risk to all stores significant enough to implement a universal, though temporary, switch to manual card-processing. P.F. Chang's later analysis (based on internal information not before the district court at this stage) led it to conclude that only 33 stores were affected. This creates a factual dispute about the scope of the breach, but it does not destroy standing. P.F. Chang's will have the opportunity to present evidence to explain how the breach occurred and which stores it affected. Perhaps it can trace which specific data files were stolen. Perhaps each individual location's data is behind a separate firewall. Or perhaps it is being too optimistic and the breach was greater than it suggests. At this stage, no one knows. When the data system for an entire corporation with locations across the country experiences a data breach and the corporation reacts

as if that breach could affect all of its locations, it is certainly plausible that all of its locations were in fact affected.

For completeness, we briefly address Lewert and Kosner's other asserted injuries. We do not decide whether any of these would be sufficient injury for Article III standing, but we are skeptical.

Plaintiffs claim that the cost of their meals is an injury because they would not have dined at P.F. Chang's had they known of its poor data security. As we noted in *Remijas*, such arguments have been adopted by courts only where the product itself was defective or dangerous and consumers claim they would not have bought it (or paid a premium for it) had they known of the defect. *Remijas*, 794 F.3d at 695; see, *e.g.*, *In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) (acknowledging financial injury when plaintiffs "paid more for the toys than they would have, had they known of the risks the beads posed to children"). The plaintiffs here make no such allegations, and we are not inclined to push this theory beyond its current scope.

Plaintiffs also claim that they have a property right to their personally identifiable data, and that the theft of their data supports standing just as well as the theft of one's car would. But the only authority to which they direct us is *Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618 (7th Cir. 2014), which says nothing of the kind. That case interpreted the Video Privacy Protection Act, 18 U.S.C. § 2710, which creates a legally protected interest in a consumer's personally identifiable information with respect to video rentals. *Id.* at 623. *Sterk* does not recognize a legal interest in personally identifiable information beyond the video-rental context.

Plaintiffs fare no better under state law. They contend that Illinois's Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505, protects their personally identifiable information by establishing that its theft is an injury even in the absence of actual damages. But the Illinois Appellate Court has held otherwise: the statute requires "actual damages" before a private litigant can bring suit. *People ex rel. Madigan v. United Constr. of America, Inc.*, 981 N.E.2d 404, 410–11 (Ill. App. Ct. 2012).

In short, at least some of the injuries Lewert and Kosner allege here qualify as immediate and concrete injuries sufficient to support Article III standing. If they can meet the other two criteria for standing, this case can go forward.

B

Those criteria are causation and redressability. See *Hollingsworth*, 133 S. Ct. at 2661. P.F. Chang's argues that the plaintiffs cannot show causation because their information was never compromised and in any event any fraudulent charges cannot be attributed to its data breach. The former argument assumes the answer to a disputed fact—whether the Northbrook restaurant was among those hit by the hackers. Plaintiffs have alleged that it was, and they have included enough facts to push that allegation to the point of plausibility. The latter argument is a theory of defense that P.F. Chang's will be entitled to pursue at the merits phase. Both P.F. Chang's and the plaintiffs have available to them the standard methods of proving causation. See *Remijas*, 794 F.3d at 696 (citing *Summers v. Tice*, 199 P.2d 1 (Cal. 1948) (*en banc*) (explaining that once a plaintiff properly pleads joint liability, the burden shifts to defendants to demonstrate re-

sponsibility)); *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring) ("the common law of torts has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury"). Merely identifying potential alternative causes does not defeat standing.

Finally, a favorable judgment would redress the plaintiffs' injuries. Kosner and those in his position, for example, have some easily quantifiable financial injuries: they purchased credit monitoring services. Kosner also alleges that he was unable to accrue points on his debit card while he was waiting for a replacement. If that loss has any monetary value (a question on which we take no position), it would be compensable. While neither Lewert nor Kosner have unreimbursed fraudulent charges on their payment cards, other class members (should the class be certified) might. See *Remijas*, 794 F.3d at 697 (explaining that federal law does not require credit and debit card companies to reimburse consumers for all fraudulent charges). And all class members should have the chance to show that they spent time and resources tracking down the possible fraud, changing automatic charges, and replacing cards as a prophylactic measure.

C

Finally, we briefly address P.F. Chang's alternative argument that the plaintiffs failed to state a claim upon which relief can be granted. FED. R. CIV. P. 12(b)(6). A dismissal for failure to state a claim is with prejudice. *Id.* The district court here dismissed the plaintiffs' claims for lack of subject-matter jurisdiction, which is a dismissal without prejudice. FED. R. CIV. P. 12(b)(1). The district court did not reach P.F.

Chang's arguments about failure to state a claim. While we may affirm a judgment on an alternative ground, *Hester v. Indiana State Department of Health*, 726 F.3d 942, 946 (7th Cir. 2013), we may do so only when that ground supports the same relief. We may not grant additional relief unless the appellee files a cross-appeal. As the Supreme Court explained in *Jennings v. Stephens*, "an appellee who does not cross-appeal may not attack the decree with a view either to enlarging his own rights thereunder or of lessening the rights of his adversary." 135 S. Ct. 793, 798 (2015) (internal quotation marks omitted). Because P.F. Chang's did not file a cross—appeal, we cannot and do not consider whether the plaintiffs failed to state a claim.

We conclude that the plaintiffs have alleged enough to support Article III standing. In so ruling, we express no opinion on the merits or on the suitability of this case for class certification. The district court's judgment is REVERSED and the case REMANDED for further proceedings consistent with this opinion.