

In the
United States Court of Appeals
For the Seventh Circuit

No. 14-3122

HILARY REMIJAS, on behalf of herself and all others similarly
situated, *et al.*,

Plaintiffs-Appellants,

v.

NEIMAN MARCUS GROUP, LLC,

Defendant-Appellee.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 14 C 1735 — **James B. Zagel**, *Judge*.

ARGUED JANUARY 23, 2015 — DECIDED JULY 20, 2015

Before WOOD, *Chief Judge*, and KANNE and TINDER, *Circuit Judges*.

WOOD, *Chief Judge*. Sometime in 2013, hackers attacked Neiman Marcus, a luxury department store, and stole the credit card numbers of its customers. In December 2013, the company learned that some of its customers had found fraudulent charges on their cards. On January 10, 2014, it announced to the public that the cyberattack had occurred

and that between July 16, 2013, and October 30, 2013, approximately 350,000 cards had been exposed to the hackers' malware. In the wake of those disclosures, several customers brought this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), seeking various forms of relief. The district court stopped the suit in its tracks, however, ruling that both the individual plaintiffs and the class lacked standing under Article III of the Constitution. This resulted in a dismissal of the complaint without prejudice. See *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 102 (1998) (standing to sue is a threshold jurisdictional question); *Hernandez v. Conriv Realty Assocs.*, 182 F.3d 121, 122 (2d Cir. 1999) (“[W]here federal subject matter jurisdiction does not exist, federal courts do not have the power to dismiss with prejudice”). We conclude that the district court erred. The plaintiffs satisfy Article III's requirements based on at least some of the injuries they have identified. We thus reverse and remand for further proceedings.

I

In mid-December 2013, Neiman Marcus learned that fraudulent charges had shown up on the credit cards of some of its customers. Keeping this information confidential at first (according to plaintiffs, so that the breach would not disrupt the lucrative holiday shopping season), it promptly investigated the reports. It discovered potential malware in its computer systems on January 1, 2014. Nine days later, it publicly disclosed the data breach and sent individual notifications to the customers who had incurred fraudulent charges. The company also posted updates on its website. Those messages confirmed several aspects of the attack: some card numbers had been exposed to the malware, but

No. 14-3122

3

other sensitive information such as social security numbers and birth dates had not been compromised; the malware attempted to collect card data between July 16, 2013, and October 30, 2013; 350,000 cards were potentially exposed; and 9,200 of those 350,000 cards were known to have been used fraudulently. Notably, other companies had also suffered cyberattacks during that holiday season.

At that point, Neiman Marcus notified all customers who had shopped at its stores between January 2013 and January 2014 and for whom the company had physical or email addresses, offering them one year of free credit monitoring and identity-theft protection. On February 4, 2014, Michael Kingston, the Senior Vice President and Chief Information Officer for the Neiman Marcus Group, testified before the United States Senate Judiciary Committee. He represented that “the customer information that was potentially exposed to the malware was payment card account information” and that “there is no indication that social security numbers or other personal information were exposed in any way.”

These disclosures prompted the filing of a number of class-action complaints. They were consolidated in a First Amended Complaint filed on June 2, 2014, by Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao. They sought to represent themselves and the approximately 350,000 other customers whose data may have been hacked. The complaint relies on a number of theories for relief: negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws. It raises claims that exceed \$5,000,000, and minimal diversity of citizenship exists, because Remijas is a citizen of Illinois, Frank is a citi-

zen of New York, and Farnoush and Kao are citizens of California, while the Neiman Marcus Group LLC, once ownership is traced through several intermediary LLCs, is owned by NM Mariposa Intermediate Holdings Inc., a Delaware corporation with its principal place of business in Texas. The district court's jurisdiction (apart from the Article III issue to which we will turn) was therefore proper under 28 U.S.C. § 1332(d)(2).

Remijas alleged that she made purchases using a Neiman Marcus credit card at the department store in Oak Brook, Illinois, in August and December 2013. Frank alleged that she and her husband used a joint debit card account to make purchases at a Neiman Marcus store on Long Island, New York, in December 2013; that on January 9, 2014, fraudulent charges appeared on her debit card account; that, several weeks later, she was the target of a scam through her cell phone; and that her husband received a notice letter from Neiman Marcus about the breach. Farnoush alleged that she also incurred fraudulent charges on her credit card after she used it at Neiman Marcus in 2013. Finally, Kao made purchases on ten separate occasions at a Neiman Marcus store in San Francisco in 2013 and received notifications in January 2014 from her bank as well as Neiman Marcus that her debit card had been compromised.

Citing Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), Neiman Marcus moved to dismiss the complaint for lack of standing and for failure to state a claim. On September 16, 2014, the district judge granted the motion exclusively on standing grounds, and the plaintiffs filed their notice of appeal nine days later. This created a slight problem with appellate jurisdiction, because the district judge never set

No. 14-3122

5

out his judgment in a separate document as required by Rule 58(a). Nonetheless, we have confirmed that there is a final judgment for purposes of 28 U.S.C. § 1291 and our jurisdiction is secure. (This step would not be necessary if the district court had taken the simple additional step described in Rule 58(a); we once again urge the district courts to do so, for the sake of both the parties and the appellate court.) Here, the district court clearly evidenced its intent in its opinion that this was the final decision in the case, and the clerk recorded the dismissal in the docket. *Bankers Trust Co. v. Mallis*, 435 U.S. 381, 387–88 (1978); see also *Kaplan v. Shure Bros.*, 153 F.3d 413, 417 (7th Cir. 1998). As neither party has called to our attention anything that would defeat finality nor do we see anything, we are free to proceed.

II

We review a district court's dismissal for lack of Article III standing *de novo*. *Reid L. v. Ill. State Bd. of Educ.*, 358 F.3d 511, 515 (7th Cir. 2004). Under Rule 12(b)(1), "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 parties invoking federal jurisdiction, bear the burden of establishing the required elements of standing." *Id.* (citation omitted); see *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). In order to have standing, a litigant must "prove that he has 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).

These plaintiffs must allege that the data breach inflicted concrete, particularized injury on them; that Neiman Marcus caused that injury; and that a judicial decision can provide redress for them. We first address these requirements of Article III standing, and then briefly comment on Neiman Marcus's argument that, alternatively, the complaint should be dismissed for failure to state a claim.

A

The plaintiffs point to several kinds of injury they have suffered: 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information. (We note that these allegations go far beyond the complaint about a website's publication of inaccurate information, in violation of the Fair Credit Reporting Act, that is before the Supreme Court in *Spokeo, Inc. v. Robins*, No. 13-1339, *cert. granted* 135 S. Ct. 1892 (2015).) The plaintiffs also allege that they have standing based on two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft. We address the two alleged imminent injuries first and then the four asserted actual injuries.

Allegations of future harm can establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (citation omitted). Here, the complaint alleges that everyone's personal data has already been stolen; it alleges that the 9,200 who already

No. 14-3122

7

have incurred fraudulent charges have experienced harm. Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges. The complaint also alleges a concrete risk of harm for the rest. The question is whether these allegations satisfy *Clapper's* requirement that injury either already have occurred or be "certainly impending."

As for the 9,200 (including Frank and Farnoush), the plaintiffs concede that they were later reimbursed and that the evidence does not yet indicate that their identities (as opposed to the data) have been stolen. But as we already have noted, there are identifiable costs associated with the process of sorting things out. Neiman Marcus challenges the standing of these class members, but we see no merit in that point. What about the class members who contend that unreimbursed fraudulent charges and identity theft may happen in the future, and that these injuries are likely enough that immediate preventive measures are necessary? Neiman Marcus contends that this is too speculative to serve as injury-in-fact. It argues that all of the plaintiffs would be reimbursed for fraudulent charges because (it asserts) that is the common practice of major credit card companies. The plaintiffs disagree with the latter proposition; they contend that they, like all consumers subject to fraudulent charges, must spend time and money replacing cards and monitoring their credit score, and that full reimbursement is not guaranteed. (It would not be enough to review one's credit card statements carefully every month, because the thieves might—and often do—acquire new credit cards unbeknownst to the victim.) This reveals a material factual dispute on such mat-

ters as the class members' experiences and both the content of, and the universality of, bank reimbursement policies.

Clapper does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing. In *Clapper*, the Supreme Court decided that human rights organizations did not have standing to challenge the Foreign Intelligence Surveillance Act (FISA) because they could not show that their communications with suspected terrorists *were* intercepted by the government. The plaintiffs only suspected that such interceptions might have occurred. This, the Court held, was too speculative to support standing. In so ruling, however, it did not jettison the "substantial risk" standard. To the contrary, it stated that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." 133 S. Ct. at 1150 n.5 (2013) (citation omitted).

In a data breach case similar to ours, a district court persuasively applied these principles, including *Clapper's* recognition that a substantial risk will sometimes suffice to support Article III standing. "Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real." *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *8 (N.D. Cal. Sept. 4, 2014) (citing *Clapper*, 133 S. Ct. at 1148). Our case is much the same. The plaintiffs allege that the

No. 14-3122

9

hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information. Whereas in *Clapper*, “there was no evidence that any of respondents’ communications either had been or would be monitored,” in our case there is “no need to speculate as to whether [the Neiman Marcus customers’] information has been stolen and what information was taken.” *Id.* (citing *Clapper*, 133 S. Ct. at 1148). Like the *Adobe* plaintiffs, the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an “objectively reasonable likelihood” that such an injury will occur. *Clapper*, 133 S. Ct. at 1147.

Requiring the plaintiffs “to wait for the threatened harm to materialize in order to sue” would create a different problem: “the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not ‘fairly traceable’ to the defendant’s data breach.” *In re Adobe Sys.*, 2014 WL 4379916, at *8 n.5. Neiman Marcus has made just that argument here. The point is best understood as a challenge to the causation requirement of standing, to which we turn shortly.

At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities. The plaintiffs are also careful to say that only 9,200 cards have experienced fraudulent charges *so far*; the complaint asserts that fraudulent charges and identity theft can occur long after a data breach. It cites a Government Ac-

countability Office Report that finds that “stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.” U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007). (This suggests that on remand the district court may wish to look into length of time that a victim is truly at risk; the GAO suggests at least one year, but more data may shed light on this question.) We recognize that the plaintiffs may eventually not be able to provide an adequate factual basis for the inference, but they had no such burden at the pleading stage. Their allegations of future injury are sufficient to survive a 12(b)(1) motion.

In addition to the alleged future injuries, the plaintiffs assert that they have already lost time and money protecting themselves against future identity theft and fraudulent charges. Mitigation expenses do not qualify as actual injuries where the harm is not imminent. *Clapper*, 133 S. Ct. at 1152 (concluding that “costs that they have incurred to avoid [injury]” are insufficient to confer standing). Plaintiffs “cannot manufacture standing by incurring costs in anticipation of non-imminent harm.” *Id.* at 1155. “If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” *Id.* at 1151.

Once again, however, it is important not to overread *Clapper*. *Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected

No. 14-3122

11

customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for \$4.95 a month for the first month, and then \$19.95 per month thereafter. See <http://www.experian.com/consumer-products/credit-monitoring.html>. That easily qualifies as a concrete injury. It is also worth noting that our analysis is consistent with that in *Anderson v. Hannaford Bros. Co.*, where the First Circuit held before *Clapper* that the plaintiffs sufficiently alleged mitigation expenses—namely, the fees for replacement cards and monitoring expenses—because under Maine law, a plaintiff may “recover for costs and harms incurred during a reasonable effort to mitigate, regardless of whether the harm is non-physical.” 659 F.3d 151, 162 (1st Cir. 2011).

For the sake of completeness, we comment briefly on the other asserted injuries. They are more problematic. We need not decide whether they would have sufficed for standing on their own, but we are dubious. The plaintiffs argue, for example, that they overpaid for the products at Neiman Marcus because the store failed to invest in an adequate security system. In some situations, we have held that financial injury in the form of an overcharge can support Article III standing. See *In re Aqua Dots Products Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) (“The plaintiffs’ loss is financial: they

paid more for the toys than they would have, had they known of the risks the beads posed to children. A financial injury creates standing.”) (citations omitted). District courts have applied this approach to comparable situations. See, e.g., *Chicago Faucet Shoppe, Inc. v. Nestle Waters N. Am. Inc.*, No. 12 C 08119, 2014 WL 541644, at *3 (N.D. Ill. Feb. 11, 2014) (citing *Aqua Dots*); *Muir v. Playtex Products, LLC*, 983 F. Supp. 2d 980, 986 (N.D. Ill. 2013) (holding that a claim that consumer would not have purchased product or not have paid a premium price for the product is sufficient injury to establish standing).

Importantly, many of those cases involve products liability claims against defective or dangerous products. See, e.g., *Lipton v. Chattem, Inc.* No. 11 C 2952, 2012 WL 1192083, at *3–4 (N.D. Ill. Apr. 10, 2012). Our case would extend that idea from a particular product to the operation of the entire store: plaintiffs allege that they would have shunned Neiman Marcus had they known that it did not take the necessary precautions to secure their personal and financial data. They appear to be alleging some form of unjust enrichment as well: Neiman Marcus sold its products at premium prices, but instead of taking a portion of the proceeds and devoting it to cybersecurity, the company pocketed too much. This is a step that we need not, and do not, take in this case. Plaintiffs do not allege any defect in any product they purchased; they assert instead that patronizing Neiman Marcus inflicted injury on them. Compare *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (reasoning that the plaintiff had financial injury from paying higher premiums in light of defendant’s failure to implement security policies). That allegation takes nothing away from plaintiffs’ more concrete alle-

No. 14-3122

13

gations of injury, but it is not necessary to support their standing.

The plaintiffs also allege that they have a concrete injury in the loss of their private information, which they characterize as an intangible commodity. Under this theory, persons who had unauthorized credit charges would have standing even if they were automatically reimbursed, their identities were not stolen, and they could not show that there was a substantial risk of lack of reimbursement or further use of their information. This assumes that federal law recognizes such a property right. Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.

The plaintiffs counter that recently-enacted state statutes make this right to personal information concrete enough for standing. They are correct to the extent they suggest that “the actual or threatened injury required under Article III can be satisfied solely by virtue of an invasion of a recognized state-law right.” *Scanlan v. Eisenberg*, 669 F.3d 838, 845 (7th Cir. 2012) (citation omitted). The plaintiffs argue that Neiman Marcus violated California and Illinois’s Data Breach Acts by impermissibly delaying the notifications of the data breach. That may be (we express no opinion on the point), but even if it is, the violation does not help the plaintiffs. Neither of those statutes provides the basis for finding an injury for Article III standing. As for California law, a delay in notification is not a cognizable injury, *Price v. Starbucks Corp.*, 192 Cal. App. 4th 1136, 1143 (Cal. Ct. App. 2011), and the Illinois Consumer Fraud Act requires “actual damages.”

People ex rel. Madigan v. United Constr. of Am., Inc., 981 N.E.2d 404, 411 (Ill. App. Ct. 2012). None of the other state-law claims has been discussed by the parties, and so we too do not address them.

To sum up, we refrain from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III. The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft do. These injuries are sufficient to satisfy the first requirement of Article III standing.

B

Injury-in-fact is only one of the three requirements for Article III standing. Plaintiffs must also allege enough in their complaint to support the other two prerequisites: causation and redressability. As the Supreme Court put it in *Clapper*, plaintiffs must "show[] that the defendant's actual action has caused the substantial risk of harm." 133 S. Ct. at 1150, n.5. Neiman Marcus argues that these plaintiffs cannot show that their injuries are traceable to the data incursion at the company rather than to one of several other large-scale breaches that took place around the same time. This argument is reminiscent of *Summers v. Tice*, 199 P.2d 1, 5 (Cal. 1948), in which joint liability was properly pleaded when, during a quail hunt on the open range, the plaintiff was shot, but he did not know which defendant had shot him. Under those circumstances, the Supreme Court of California held, the burden shifted to the defendants to show who was responsible. Neiman Marcus apparently rejects such a rule, but we think that this debate has no bearing on standing to sue;

No. 14-3122

15

at most, it is a legal theory that Neiman Marcus might later raise as a defense.

The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are "fairly traceable" to the data breach at Neiman Marcus. See *In re Target Corp. Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014) ("Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue."). If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then "the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J. concurring) (citing *Summers*, 199 P.2d at 3-4). It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level. See *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

With respect to standing, Neiman Marcus finally argues that the plaintiffs' injuries cannot be redressed by a judicial decision because they already have been reimbursed for the fraudulent charges. That may be true for the fraudulent

charges (the plaintiffs do not allege that any of those charges went unreimbursed), but it is not true for the mitigation expenses or the future injuries. Although some credit card companies offer some customers “zero liability” policies, under which the customer is not held responsible for any fraudulent charges, that practice defeats neither injury-in-fact nor redressability. The “zero liability” feature is a business practice, not a federal requirement. Under 15 U.S.C. § 1643, a consumer’s liability for the unauthorized use of her credit card may not exceed \$50 if she does not report the loss before the credit card is used. If she notifies the card issuer before any use, she is not responsible for any charges she did not authorize. Debit cards (used by several of the named plaintiffs) receive less protection than credit cards; the former are covered under the Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*, and the latter under the Truth in Lending Act as amended by the Fair Credit Billing Act, 15 U.S.C. § 1601 *et seq.* If a person fails to report to her bank that money has been taken from her debit card account more than 60 days after she receives the statement, there is no limit to her liability and she could lose all the money in her account. In any event, as we have noted, reimbursement policies vary. For the plaintiffs, a favorable judicial decision could redress any injuries caused by less than full reimbursement of unauthorized charges.

C

Neiman Marcus attempts to argue in the alternative that the plaintiffs failed to state a claim upon which relief can be granted. FED. R. CIV. P. 12(b)(6). Their problem is that the district court did not reach this ground, and that the ground on which it resolved the case (Article III standing) necessarily

No. 14-3122

17

resulted in a dismissal without prejudice. A dismissal under Rule 12(b)(6), in contrast, is a dismissal with prejudice. If Neiman Marcus had wanted this additional relief, it needed to file a cross-appeal. See *Jennings v. Stephens*, 135 S. Ct. 793, 798 (2015) (“[A]n 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.”) (citation and quotation marks omitted). Since it did not, the question whether this complaint states a claim on which relief can be granted is not properly before us.

We therefore conclude that the plaintiffs have adequately alleged standing under Article III. The district court’s judgment is REVERSED and the case is REMANDED for further proceedings consistent with this opinion.