Case No. 14-3122

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

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

Plaintiffs-Appellants,

v.

THE NEIMAN MARCUS GROUP LLC, a Delaware limited liability company,

Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of Illinois,
Case No. 1:14-cv-01735, Hon. James B. Zagel

PETITION FOR REHEARING EN BANC

David H. Hoffman
Tacy F. Flint
Daniel C. Craig
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000

Attorneys for Defendant-Appellee

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 14-3122

Short Caption: Remijas v. The Neiman Marcus Group LLC

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

The Neiman Marcus Group LLC

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Sidley Austin LLP

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

Neiman Marcus Group LTD LLC

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

N/A

Attorney's Signature: s/ David H. Hoffman Date: 8/3/2015

Attorney's Printed Name: David H. Hoffman

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** X **No** _____

Address: Sidley Austin LLP
One South Dearborn, Chicago, IL 60603

Phone Number: 312-853-2174 Fax Number: 312-853-7036

E-Mail Address: david.hoffman@sidley.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 14-3122

Short Caption: Remijas v. The Neiman Marcus Group LLC

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

The Neiman Marcus Group LLC

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Sidley Austin LLP

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

Neiman Marcus Group LTD LLC

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

N/A

Attorney's Signature: s/ Tacy F. Flint Date: 8/3/2015

Attorney's Printed Name: Tacy F. Flint

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: Sidley Austin LLP
One South Dearborn, Chicago, IL 60603

Phone Number: 312-853-7875 Fax Number: 312-853-7036

E-Mail Address: tflint@sidley.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 14-3122

Short Caption: Remijas v. The Neiman Marcus Group LLC

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

The Neiman Marcus Group LLC

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Sidley Austin LLP

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

Neiman Marcus Group LTD LLC

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

N/A

Attorney's Signature: s/ Daniel C. Craig Date: 8/3/2015

Attorney's Printed Name: Daniel C. Craig

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: Sidley Austin LLP
One South Dearborn, Chicago, IL 60603

Phone Number: 312-853-7370 Fax Number: 312-853-7036

E-Mail Address: dcraig@sidley.com

TABLE OF CONTENTS

GROUNDS FOR REHEARING CASE EN BANC 1

STATEMENT OF CASE AND SUMMARY OF PROCEEDINGS 2

ARGUMENT 5

I. The Panel Used a Standard Explicitly Rejected By the Supreme Court to Hold That Mere Speculation of Future Injury Confers Standing. 6

II. The Panel Further Departed from the Supreme Court in Relying on Speculation and Conjecture—Rather Than Concrete Factual Allegations—to Assess Injury. 9

III. The Court's Decision Creates a Split With the Third Circuit and Is Against the Very Substantial Weight of District Court Decisions. 13

CONCLUSION 15

TABLE OF AUTHORITIES

Page(s)

Cases

In re Adobe Sys., Inc. Privacy Litig.,
66 F. Supp. 3d 1197, 1206, 1215 (N.D. Cal. 2014) 10

Allison v. Aetna, Inc.,
No. 09-2560, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010) 15

Amburgy v. Express Scripts, Inc.,
671 F. Supp. 2d 1046 (E.D. Mo. 2009) 15

Anderson v. Hannaford Bros. Co.
659 F.3d 151, 154, 167 (1st Cir. 2011) 12

In re Barnes & Noble Pin Pad Litig.,
No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) 15

Burton v. Mapco Express, Inc.,
47 F. Supp. 3d 1279, 1284-85 (N.D. Ala. 2014) 15

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013) .... *passim*

Galaria v. Nationwide Mut. Ins. Co.,
998 F. Supp. 2d 646 (S.D. Ohio 2014) 15

Hammond v. Bank of New York Mellon Corp.,
No. 08 Civ. 6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010) 15

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 1, 11

Monsanto Co. v. Geertson Seed Farms,
561 U.S. 139 (2010) 8

Pennsylvania v. West Virginia,
262 U.S. 553 (1923) 11

Reilly v. Ceridian Corp.,
664 F.3d 38 (3d Cir. 2011) 2, 14, 15

In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,
45 F. Supp. 3d 14, 25 (D.D.C. 2014) 15

Strautins v. Trustwave Holdings, Inc.,
27 F. Supp. 3d 871, 875 (N.D. Ill. 2014) 15

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014) 8, 10

Warth v. Seldin,
422 U.S. 490 (1975) 1, 10, 12, 13

Whitmore v. Arkansas,
495 U.S. 149 (1990) 1, 11

Other Authorities

FTC, *Protecting Against Credit Card Fraud*,
http://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud (accessed Aug. 3, 2015) 13

Judy Greenwald, *Neiman Marcus Cyber Security Ruling Could Have Wide Influence*, Bus. Insurance (July 28, 2015) 6

Zuzana S. Ikels, *Privacy Takeaways from the Neiman Marcus Breach Case*,
Law360 (Aug. 3, 2015) 6

Nathaniel Popper, *Stolen Consumer Data Is A Smaller Problem Than It Seems*,
N.Y. Times BU6 (July 31, 2015) 5

Priya Roy, *A Standing Ovation for Plaintiffs in Data Breach Cases*, Law360 (July 27, 2015) 6

GROUNDS FOR REHEARING CASE EN BANC

1. The panel's opinion squarely conflicts with the most recent and controlling decisions of the Supreme Court regarding the Article III requirement of a cognizable injury.

a. The panel held that there is standing when the "likelihood" of future injury (here, future identity theft or credit card fraud) is "objectively reasonable." Op. at 9. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), explicitly rejected an "objectively reasonable likelihood test, holding that it was "inconsistent" with the Court's requirement that a potential future injury be "imminent" and "certainly impending." The panel's ruling here is thus squarely at odds with Supreme Court precedent. *See* Section I, *infra*.

b. In addition, the record before the district court made clear that there was no risk—and the plaintiffs did not allege— that they would be financially responsible for any fraudulent credit card charges. The panel ignored that evidence, and even twisted action by Neiman Marcus to protect its customers into actual harm suffered by the plaintiffs. The panel further ignored the fact that security incidents like this one involving payment card data—not other personal data like Social Security numbers—create no meaningful risk of identity theft. The panel instead relied on speculative and conjectural observations—nowhere alleged by plaintiffs—in an analysis that conflicts with two lines of Supreme Court precedent regarding Article III standing: (i) cases holding that Article III standing cannot be based on speculation and conjecture but requires concrete and particularized injuries that are actual or imminent,[1] and (ii) cases holding that plaintiffs bear the burden of alleging specific, concrete facts that establish Article III standing.[2] *See* Section II, *infra*.

2. This case also involves questions of exceptional importance:

---

[1] *See, e.g.*, *Clapper*, 133 S. Ct. at 1147; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990).
[2] *See, e.g.*, *Clapper*, 133 S. Ct. at 1146, 1150 n. 5; *Warth v. Seldin*, 422 U.S. 490, 508 (1975).

a. This Court is now the first court of appeals to address squarely the issue of standing in the context of payment-card data breaches, at a time when data breaches—and resulting litigation—are exploding in number. No company or governmental institution is immune. The panel's use of an expansive standard to find that conclusory, speculative allegations of future and present injury suffice under Article III is thus enormously consequential to the national legal landscape. While some data breaches may pose actual risk of imminent identity theft and future injury, the panel's loose thinking about the risks of a breach limited to payment cards simply does not comply with Supreme Court precedent and would expand federal jurisdiction to cases in which no actual or imminent injury exists, ignoring the Supreme Court's frequent declaration that "no principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Clapper*, 133 S. Ct. at 1146. *See* Argument Intro., *infra*.

b. The panel's opinion creates a circuit split with the Third Circuit. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011), and is against the very substantial weight of district court decisions. *See* Section III, *infra*.

STATEMENT OF CASE AND SUMMARY OF PROCEEDINGS

In January and February 2014, Neiman Marcus discovered and publicly announced that it had been subjected to a cyber-security attack in which malicious software ("malware") had been inserted in its computer systems. As a result, approximately 350,000 payment card accounts used at certain Neiman Marcus stores between July 16 and October 30, 2013 were potentially compromised. It also announced that it had been notified that fraudulent charges had appeared on approximately 9,200 of these payment cards.

Four individual plaintiffs sued Neiman Marcus on behalf of a putative class. None of the plaintiffs alleged any *unreimbursed* fraudulent charges. Only one, Melissa Frank, alleged that

she had used her payment card at Neiman Marcus during the specific period when the malware was operating, and had subsequently experienced a fraudulent charge on her payment card—though like the other plaintiffs, Ms. Frank did not allege that she was held financially responsible for the charge. Neiman Marcus moved to dismiss the complaint under Rule 12(b)(1), on the ground that none of the plaintiffs could demonstrate injury sufficient to establish standing under Article III. In support of its motion, Neiman Marcus submitted evidence that all fraudulent charges that appeared on payment cards had been and would be reimbursed by the card issuers. R. 36-1: 5, 19. The district court granted the motion, holding that none of the plaintiffs had shown either actual injury or imminent future injury.

The district court explained that the plaintiffs had alleged two future injuries: risk of future fraudulent charges, and risk of future identity theft. The court observed that under the Supreme Court's standing doctrine, future injuries must be "certainly impending" in order to satisfy Article III. D. Ct. Op. at 2–3 (quoting *Clapper*, 133 S. Ct. at 1147). Here, the supposed risk of future charges did not support standing because there was no allegation that any plaintiff had been or would be held financially responsible for any fraudulent charges. D. Ct. Op. at 6. Regarding the risk of identity theft in these circumstances—where only payment card data, not more sensitive information such as Social Security numbers, had been exposed—the court held that the mere possibility of identity theft did not satisfy Article III. *Id.* at 6–7.

The district court also concluded that neither of the plaintiffs' two alleged present injuries could support standing. First, it rejected the notion that lost "time clearing up [fraudulent] charges" constituted a concrete injury, stating that "[w]ithout a more detailed description of some fairly substantial attendant hardship, I cannot agree with Plaintiffs that such 'injuries' confer Article III standing." *Id.* at 6. Second, the court held that "expenses and/or time spent on credit

monitoring and identity theft insurance" could not confer standing because plaintiffs cannot manufacture standing by spending time and money to avoid a non-imminent risk. *Id.* at 7–8.

A panel of this Court reversed. It concluded that the alleged future injuries—the risk of future fraudulent charges and identity theft—supported standing, stating that "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*." Op. at 9 (quoting *Clapper*, 133 S. Ct. at 1147) (emphasis added). That the plaintiffs' allegations provided no reason to believe they would suffer future unreimbursed charges was irrelevant to the panel. The panel speculated that they were likely enough to occur anyway, because "full reimbursement *is not guaranteed*," and (ii) "thieves might—and often do—acquire new credit cards unbeknownst to the victim." *Id.* at 7 (emphasis added). Similarly, with respect to the bare possibility of future identity theft, the panel observed that "fraudulent charges and identity theft *can occur* long after a data breach." *Id.* at 9 (emphasis added). The panel "recognize[d] that the plaintiffs may eventually not be able to provide an adequate factual basis for the inference" that they faced a latent risk of identity theft, but stated that plaintiffs "had no such burden at the pleading stage." *Id.* at 10.

As to the two alleged present injuries, the panel concluded that "time and money resolving fraudulent charges" conferred standing. *Id.* at 6-7. The panel recognized the plaintiffs' concession that they had been reimbursed for any fraudulent charges and that there was no indication of any identity theft, but concluded that "there are identifiable costs associated with the process of sorting things out," even though plaintiffs had not alleged anything concrete or specific about costs of "sorting things out." *Id.* at 7. The panel also concluded that "time and money protecting themselves against future identity theft and fraudulent charges" conferred

standing, based on the fact that Neiman Marcus had voluntarily supplied its customers one year of free credit monitoring and identity-theft protection, and that service cost *Neiman Marcus* money (citing a website listing the monthly fees charged by a credit-monitoring service not addressed by the parties). *Id.* at 10-11. The panel concluded from this that the cost of credit monitoring "easily qualifies as a concrete injury" to the *plaintiffs*, because a hypothetical Neiman Marcus customer "might think it necessary" to purchase credit monitoring despite having been offered it free of charge. *Id.* at 11.

ARGUMENT

Despite the increasing quantity and scope of data security incidents, injury to consumers remains rare, in part because card issuers promptly cancel compromised cards and reimburse any fraudulent charges that do occur.[3] Because data breaches affecting retailers do not typically (and here did not) involve sensitive information like Social Security numbers, the risk of broader identity theft from compromise of payment card data held by a retailer is small.[4] For that reason, the weight of authority, primarily in district courts, holds that plaintiffs suing retailers after data breaches like the one at issue here do not have standing to sue absent evidence of particularized harm, rather than mere allegations of fear of future injury. *Infra,* pp. 14-15.

The panel's contrary decision is remarkable. First, it is founded on clear and significant error: the panel used a standard for assessing when future harm confers standing—if there is an "objectively reasonable likelihood" of harm (Op. at 9)—that the Supreme Court explicitly rejected as "inconsistent with our requirement that 'threatened injury' must be certainly impending to constitute injury in fact." *Clapper*, 133 S. Ct. at 1147. The panel further erred by

---

[3] *See* Nathaniel Popper, *Stolen Consumer Data Is A Smaller Problem Than It Seems*, N.Y. Times BU6 (July 31, 2015).

[4] *Id.* ("[T]o commit true identity theft, hackers generally need to get a hold of Social Security numbers," according to the "program director at the Identity Theft Resource Center").

allowing generalized speculation about both the possibility of future harm and the existence of actual harm to satisfy the plaintiffs' burden to allege injury specifically and concretely.

These errors are certain to have immediate and broad impact. As the first appellate ruling squarely to address standing in the context of payment-card data breaches, the panel's ruling threatens to erode standing requirements in such cases well beyond the generally applicable limits declared by the Supreme Court. Less than two weeks out, the panel's opinion has already been cited in pending cases in multiple district courts, and has generated substantial legal commentary.[5] Despite substantial efforts by retailers and the credit card industry to prevent harm to consumers from payment-card breaches, this opinion all but declares that such breaches *automatically* confer standing. Indeed, the panel treated actions by Neiman Marcus to further *reduce* the remote risk of injury (free credit monitoring) as *evidence* of injury-in-fact. The ruling, if allowed to stand, will impose wasteful litigation burdens on retailers and the federal courts. This Court should accept review *en banc* to restore the well-established rule that federal lawsuits may not proceed until plaintiffs have alleged an actual or imminent concrete injury.

I. The Panel Used a Standard Explicitly Rejected By the Supreme Court to Hold That Mere Speculation of Future Injury Confers Standing.

The panel held that Neiman Marcus customers "should not have to wait [to sue] until hackers commit identity theft or credit-card fraud in order to give the class standing, because

[5] The decision has already been raised in the following pending cases: *FTC v. Wyndham Worldwide Corp., et al.*, No. 14-3514 (3d Cir.); *In re Barnes & Noble Pin Pad Litig.*, 1:12-cv-08617 (N.D. Ill.); *Whalen v. Michaels Stores Inc.*, No. 14-CV-7006 (E.D.N.Y.); *Smith v. Triad of Alabama, LLC*, 14-CV-324 (M.D. Ala.). Legal commentary on the decision includes the following: Judy Greenwald, *Neiman Marcus Cyber Security Ruling Could Have Wide Influence*, Bus. Insurance (July 28, 2015), ("This is certainly the first major data breach case where this kind of result has been reached."); Zuzana S. Ikels, *Privacy Takeaways from the Neiman Marcus Breach Case*, Law360 (Aug. 3, 2015) (noting that "it is difficult to reconcile a decision that saddles a single company with potential liability for someone else's crime based upon potential injuries in the future"); Priya Roy, *A Standing Ovation for Plaintiffs in Data Breach Cases*, Law360 (July 27, 2015) (panel decision is "the first court of appeals to find that the data breach plaintiffs … adequately [pled] Article III standing"; panel's analysis "raises concerns that a company's data reach response and remedial measures may be used against it as evidence of harm").

there is an 'objectively reasonable likelihood' that such an injury will occur." Op. at 9 (quoting *Clapper*, 133 S. Ct. at 1147). But, when it comes to standing based on the possibility of future injury, *Clapper* explicitly *rejected* "the objectively reasonable likelihood" standard on which the panel relied.

In *Clapper*, the Court restated the traditional standing test—"an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling"—and then discussed the importance of the "imminence" element:

> Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending. Thus, we have repeatedly reiterated that threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient.

Id. at 1147 (emphasis in original; internal quotation marks, citations, and bracket omitted). The Court then rejected the test used by the Second Circuit—the "objectively reasonable likelihood" test—calling it a "novel view of standing" and holding that it was "inconsistent with our requirement that 'threatened injury' must be certainly impending to constitute injury in fact." *Id.*

The panel here simply misread *Clapper*. The panel's holding that plaintiffs "should not have to wait" to bring suit any time there is an "'objectively reasonable likelihood'" of some future harm, Op. at 9, rejects the limits on standing that *Clapper* declared. As *Clapper* held, "allegations of *possible* future injury"—even reasonably likely future injury—"are not sufficient." 133 S. Ct. at 1147 (emphasis in original). By misreading *Clapper* on this fundamental point, and by using a rejected test that is "inconsistent" with the Supreme Court's actual standing test, the panel committed clear error.

Moreover, the panel's error was essential to its ultimate holding. The question at the heart of this case is whether federal jurisdiction extends to plaintiffs who can presently allege

nothing more than a possibility of future harm, or whether federal jurisdiction requires that plaintiffs wait until actual, concrete injury has occurred or is demonstrably imminent.[6] In assessing the sufficiency of the alleged future injuries, the panel asked the wrong question. Rather than asking whether the plaintiffs' alleged future injuries were "concrete" or "imminent" or "certainly impending"—as required by Supreme Court precedent—the panel asked whether there was an "objectively reasonable likelihood" they would occur. The Supreme Court has held this is too lenient a standard, and therefore the panel's conclusion that the plaintiffs "should not have to wait" was wrong. As the Supreme Court said in *Clapper*, "no principle is more fundamental to the judiciary's proper role in our system of government." 133 S. Ct. at 1146. By using an obviously wrong and overly lenient standard to determine whether the plaintiffs' alleged future injuries provided standing, the panel committed a critical error.

---

[6] In some instances, the Supreme Court has held the imminence requirement satisfied based on a "substantial risk" of future injury. *See Clapper*, 130 S. Ct. at 1150 n.5. For instance, a unanimous Supreme Court held last year that two advocacy organizations had standing to challenge a state law criminalizing the making of a false statement about a political candidate's voting record because the organizations had already been subjected to potential sanctions under the law after a public official they had criticized brought a complaint against them, and on that basis the organizations alleged that their speech had been chilled. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2338–40 (2014). The Court reiterated that, when an individual is subject to the threatened enforcement of the law, the individual does not have to wait to be arrested or prosecuted as long as the threatened enforcement is sufficiently imminent. *Id.* at 2342. In such a case, the threat of future injury is *itself* a present injury, *id.* at 2343, and a case or controversy plainly exists. *See also Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153–54 (2010) (substantial risk that farmers' non-genetically-modified crops would be contaminated by pollen from neighboring genetically-modified crops immediately decreased value of crops, an actual injury, since it prevented farmers from marketing crops as non-genetically-modified without further testing, requiring them to take steps to minimize the risk of contamination). That description plainly does not apply here—a dispute between a merchant and some of its customers—where the plaintiffs cannot plausibly allege that the mere threat of fraudulent charges or identity theft is itself an *actual* injury.

II. The Panel Further Departed from the Supreme Court in Relying on Speculation and Conjecture—Rather Than Concrete Factual Allegations—to Assess Injury.

The panel's holdings regarding the plaintiffs' alleged injuries also conflict with Supreme Court precedent requiring that standing not be based on hypothetical, conjectural, or speculative injury claims. For instance, in discussing the risk that the plaintiffs would face future fraudulent charges on their credit or debit cards, the panel acknowledged the plaintiffs' concession that all fraudulent charges they had faced to date had been fully reimbursed. Op. at 7. Yet that fact—as well as the uncontroverted sworn testimony submitted by Neiman Marcus that "[t]he policies of payment card brands protect our customers from any liability for any unauthorized charges if the fraudulent charges are reported in a timely manner," R. 36-1: 5, 19—made no difference to the panel. The panel concluded that the plaintiffs' supposed fear of future fraudulent charges could support standing on the grounds that (i) the plaintiffs contended that "full reimbursement is not guaranteed" (a point not pled in the plaintiffs' complaint or supported by evidence) and (ii) "thieves might—and often do—acquire new credit cards unbeknownst to the victim." Op. at 7.

However, both of these conclusions rest exclusively on speculation—*i.e.*, the notion that such outcomes represent "*possible* future injury." *See Clapper*, 133 S. Ct. at 1147 (emphasis in original). To say that reimbursement of potential future fraudulent charges is "not guaranteed," or that thieves "might" do something, is simply to say that future harm is possible. There is simply no reason to believe—from the complaint's allegations, from the evidence submitted by Neiman Marcus, and from "common experience" (as the district court said, D. Ct. Op. at 6)—that these plaintiffs will experience *unreimbursed* fraud on their cards. As *Clapper* makes clear, such allegations "are not sufficient." 133 S. Ct. at 1147.

The panel compounded its error in holding that these conjectures create a "material factual dispute" regarding "the class members' experiences"[7] and "the content of, and the universality of, bank reimbursement policies." Op. at 7–8. But this ignores the Supreme Court's dictate that it is the *plaintiffs' burden* to satisfy the court of their standing, not simply to surmise that anything is possible in order to claim a "material factual dispute." *See, e.g., Susan B. Anthony List*, 134 S. Ct. at 2342*; Clapper*, 133 S. Ct. at 1147; *Whitmore*, 495 U.S. at 155.

Similarly, neither the plaintiffs nor the panel provide any reason to believe that the plaintiffs are at imminent risk of having their identity stolen. The panel has confused payment-card information with the more sensitive personal identifying information that can lead to identity theft, which is not at issue here. The panel leaned for support on a decision from the Northern District of California, in which Adobe Systems acknowledged that hackers had accessed the personal information of 38 million customers including names, mailing and email addresses, login IDs and passwords, and payment card data. *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1206, 1215 (N.D. Cal. 2014). From this, the *Adobe* court concluded without further analysis that "the danger that Plaintiffs' stolen data will be subject to misuse" was "certainly impending." *Id.* at 1215. Here, the panel concluded that "[o]ur case is much the same," noting that the hackers "deliberately" attempted to obtain customers' credit-card information, and then holding that the alleged future injuries were sufficient under the rejected "objectively reasonable likelihood" test discussed above. Op. at 8–9. But the two decisions are far from the same because the scope and content of the breached data are substantially different.

In sum, the panel's future-harms analysis is purely conjectural and wholly inconsistent with the Supreme Court's description of the imminence requirement. For decades, the Court has

[7] No class has been certified, and standing decisions must be made solely on the individual plaintiffs' circumstances. *Warth*, 422 U.S. at 502. The possibility of future injury to putative class members aside from the named plaintiffs is irrelevant.

described imminence as a requirement that the potential future injury be "certainly impending." *See*, *e.g.*, *Clapper*, 133 S. Ct. at 1147; *Defenders of Wildlife*, 504 U.S. at 564 n.2; *Whitmore*, 495 U.S. at 1724–25; *Pennsylvania v. West Virginia*, 262 U.S. 553, 593 (1923). "Impending" means something that is about to happen. Something "certainly" impending (an adverb emphasized by the Supreme Court in its discussion of the test, *see, e.g., Lujan*, at 504 U.S. at 564 n. 2) means that it is definitely just about to happen. The conjecture about whether these plaintiffs might suffer identity theft cannot in any way be described as something that is definitely just about to happen. That is especially true where the extent of the information potentially compromised was payment card data, not sensitive personal identifying information like Social Security numbers.

The panel also erred in determining that the plaintiffs' alleged "mitigation expenses"—time and money to protect themselves from future fraudulent charges and identity theft—confer standing. Op. at 10-11. First, that ruling conflicts with the holding in *Clapper* that incurring costs to avoid a potential injury that is not certainly impending does not confer standing. 133 S. Ct. at 1151 (plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"). Since, as described above, the two risks of future injury identified by the plaintiffs are not certainly impending, their alleged costs to avoid those speculative future injuries are insufficient to confer standing under *Clapper*.

While the panel acknowledged *Clapper*'s holding that plaintiffs may not manufacture standing in this way (Op. at 10-11), it declined to apply that holding. According to the panel, "[a]n affected 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." *Id.* at 11. What a hypothetical customer "might think" is a form of speculation obviously insufficient to

confer standing, especially where the complaint contains no more than a conclusory statement that the plaintiffs had "expenses and/or time spent on credit monitoring and identity theft insurance." First Am. Comp. ¶ 104. *See Clapper*, 133 S. Ct. at 1146, 1150 n.5 (plaintiff must allege "specific, concrete facts" to meet burden of showing standing); *Warth*, 422 U.S. at 508.

Remarkably, the panel supplemented the complaint not with information relating to expenses incurred by the plaintiffs, but with expenses incurred by *Neiman Marcus*—its offer to provide credit-monitoring services and identity-theft insurance to its customers without charge for one year. The panel described Neiman Marcus's offer of these services as "telling" and concluded that because a Neiman Marcus customer who was notified that her card was at risk "might think it necessary" to purchase credit monitoring services, the cost of these services as offered by Neiman Marcus "easily qualifies as a concrete injury." Op. at 11.[8] As the evidence established, however, Neiman Marcus voluntarily offered credit monitoring to a much broader group of customers than those whose payment card data was even conceivably accessible to the malware, in order to communicate the highest degree of customer service to its customers following a cyber attack—not because any of its customers had been or imminently would be harmed. R.36-1:5. It makes little legal sense to confer standing on these plaintiffs because of expenses incurred by Neiman Marcus as a customer service measure, and the panel's holding creates an unfortunate disincentive for companies to do so in the future.

The Court's discussion of the other alleged present injury suffers from the same flaws. The plaintiffs alleged without specifics that they lost "time and money associated with resolving

[8] The Court cited to the First Circuit's decision in *Anderson v. Hannaford Bros. Co.*, a 12(b)(6) decision, but the plaintiffs there specifically alleged "actual financial losses" in that they had to pay replacement card fees when they requested that their credit cards be canceled, and had "purchased" identity theft insurance and credit monitoring services. 659 F.3d 151, 154, 167 (1st Cir. 2011). Not only was there no indication that the company purchased these services for its customers, but the court certainly did not attempt to conclude, as the panel mistakenly did here, that expenses incurred by the company for these services meant that the plaintiffs suffered an actual injury.

fraudulent charges on their cards" and "spen[t] time clearing up those charges." First Am. Comp. ¶¶ 89-90. This cannot possibly meet the Supreme Court's requirement that the plaintiffs meet their burden to allege "specific, concrete facts."

In ruling otherwise, the panel again enhanced the complaint with speculation. Even though standing must be established solely based on the circumstances of the individual named plaintiffs, *see Warth,* 422 U.S. at 502, the panel concluded that the group of 9,200 customers who experienced fraudulent charges "have suffered" both "aggravation" and loss of their time to do three things: "to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges." Op. at 7. But the four named plaintiffs here allege no specific facts indicating such injury. The panel's speculation that members of the putative class faced these problems is unmoored from the actual allegations of the complaint. And the panel's conclusion that its own speculation could support standing is in direct conflict with the Supreme Court's requirements that (i) an injury be concrete and particularized, not speculative and abstract, and (ii) a plaintiff must plead specific and concrete facts in order to meet her burden of establishing standing. Moreover, there is no reason to believe the inconvenience extends beyond the routine behavior necessary in the modern age of widespread credit card use at retailers and over the internet: *all* credit card users are routinely instructed to spend time monitoring their credit card accounts,[9] and credit cards are routinely reissued, meaning that the "aggravation" the panel rested its decision on occurs as a matter of course.

III. The Court's Decision Creates a Split With the Third Circuit and Is Against the Very Substantial Weight of District Court Decisions.

In view of the panel's departures from Supreme Court precedent, it is unsurprising that the panel's decision is equally inconsistent with those of a number of other courts, including the

[9] *See* FTC, *Protecting Against Credit Card Fraud*, online at http://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud (accessed Aug. 3, 2015).

Third Circuit. In a 2011 case involving a data breach in which a hacker accessed highly sensitive information including Social Security numbers and, in some cases, birth dates and bank account information, the Third Circuit held that the risk of identity theft was too speculative to meet the imminence requirement. *Reilly*, 664 F.3d at 42. The court found no standing, even though the facts provided stronger support for an argument that there was a substantial risk of identity theft.

The court emphasized that whether the plaintiffs experienced harm depended on the capabilities and future actions of the hacker, which the court characterized as "entirely speculative." *Id.* at 45. As the court explained, "we cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury." *Id.* at 43 (emphasis in original). In addition, the court concluded that the plaintiffs' alleged present injury of spending time and money to monitor their financial information did not confer standing, "because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims." *Id.* at 46.

The panel's decision here conflicts with *Reilly*. As in that case, the plaintiffs will suffer future injury only *if* those responsible for the data breach recorded the plaintiffs' payment card data, *if* the perpetrators succeed in using the plaintiffs' payment card data to make fraudulent charges before plaintiffs cancel their cards or receive new card numbers, and *if* those fraudulent charges are not reimbursed, or *if* the perpetrators somehow manage to steal the plaintiffs' identity even without access to their Social Security numbers and other personal data. Like *Reilly*, the plaintiffs here are at risk of identity theft only based on "hypothetical future criminal acts" by

people with unknown capabilities, access to information, and inclination to perpetrate an identity-theft fraud scheme. Yet, unlike the *Reilly* court, the panel held that the plaintiffs had standing by engaging in speculation and conjecture in describing the potential future injury, and counting as sufficient an "objectively reasonable likelihood" of future injury.[10]

Thus, if permitted to stand, the panel's decision will place this Court in conflict with the Third Circuit, as well as numerous district court decisions. Yet the panel's decision will likely prove more prominent than *Reilly* and the many district court decisions going the other way: as the only appellate decision squarely considering a retail data breach in which only payment card data is stolen, the opinion could well shape the law of standing in such cases for years to come.

CONCLUSION

For the foregoing reasons, Neiman Marcus respectfully requests that the Court grant the petition for rehearing en banc.

Respectfully submitted,

Dated: August 3, 2015

s/ David H. Hoffman

David H. Hoffman
Tacy Fletcher Flint
Daniel C. Craig
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, Il. 60603
(312) 853-7000
Attorneys for Defendant-Appellee

[10] The Court's opinion is also in conflict with most district court opinions in similar cybersecurity-intrusion cases, including two other cases from the Northern District of Illinois. *See*, *e.g.*, *Strautins v. Trustwave Holdings, Inc.,* 27 F. Supp. 3d 871, 875 (N.D. Ill. 2014)*; In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *4-6 (N.D. Ill. Sept. 3, 2013)*; Burton v. Mapco Express, Inc.*, 47 F. Supp. 3d 1279, 1284-85 (N.D. Ala. 2014); *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014); *Hammond v. Bank of New York Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010); *Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052–53 (E.D. Mo. 2009).

CERTIFICATE OF COMPLIANCE

I hereby certify that:

1. This Petition complies with the requirements of Fed. R. App. P. 32(a) and Fed. R. App. P. 32(c). The Petition complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) as modified by Circuit Rule 32(b), because it has been prepared in a proportionally spaced typeface using Microsoft Word for Windows in 12-point Times New Roman, with footnotes in 11-point Times New Roman font.

2. This Petition complies with the requirements of Fed. R. App. P. 35(b)(2) because he length of this Petition is 15 pages.

s/ David H. Hoffman
Attorney for The Neiman Marcus Group LLC
Dated: August 3, 2015

CERTIFICATE OF SERVICE

I hereby certify that on August 3, 2015, the Petition for Rehearing En Banc was filed with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the appellate CM/ECF system.

The following attorneys are registered CM/ECF users and will be served by the appellate CM/ECF system:

Joseph Siprut
SIPRUT PC
Suite 1850
17 N. State Street
Chicago, IL 60602

s/ David H. Hoffman
Attorney for The Neiman Marcus Group LLC
Dated: August 3, 2015

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

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

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

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

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-

Case: 14-3122 Document: 37 Filed: 08/03/2015 Pages: 17

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

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 nonphysical." 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-

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."

Case: 14-3122 Document: 37 Filed: 08/06/2015 Pages: 17

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;

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

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.