

NOT RECOMMENDED FOR PUBLICATION

File Name: 16a0526n.06

Nos. 15-3386/3387

**UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT**

FILED
Sep 12, 2016
DEBORAH S. HUNT, Clerk

MOHAMMAD S. GALARIA (15-3386);)
ANTHONY HANCOX (15-3387), individually and)
on behalf of all others similarly situated,)
)
Plaintiffs-Appellants,)
)
v.)
)
NATIONWIDE MUTUAL INSURANCE)
COMPANY,)
)
Defendant-Appellee.)
)

ON APPEAL FROM THE
UNITED STATES DISTRICT
COURT FOR THE SOUTHERN
DISTRICT OF OHIO

BEFORE: BATCHELDER and WHITE, Circuit Judges; LIPMAN, District Judge. *

HELENE N. WHITE, Circuit Judge. Plaintiffs Mohammad Galaria and Anthony Hancox brought these putative class actions after hackers breached the computer network of Defendant Nationwide Mutual Insurance Company and stole their personal information. In their complaints, Plaintiffs allege claims for invasion of privacy, negligence, bailment, and violations of the Fair Credit Reporting Act (FCRA). The district court dismissed the complaints, concluding that Plaintiffs failed to state a claim for invasion of privacy, lacked Article III standing to bring the negligence and bailment claims, and lacked statutory standing to bring the FCRA claims. In this consolidated appeal, Plaintiffs challenge the dismissal of the negligence, bailment, and FCRA claims. Because we conclude that Plaintiffs have Article III standing and

* The Honorable Sheryl H. Lipman, United States District Judge for the Western District of Tennessee, sitting by designation.

that the district court erred in dismissing the FCRA claims for lack of subject-matter jurisdiction, we **REVERSE** and **REMAND** for further proceedings.

I. Background

As alleged in the complaints, Nationwide is an insurance and financial-services company that maintains records containing sensitive personal information about its customers, as well as potential customers who submit their information to obtain quotes for insurance products. The data include names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers. On October 3, 2012, hackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others.

Nationwide informed Plaintiffs of the breach in a letter that advised taking steps to prevent or mitigate misuse of the stolen data, including monitoring bank statements and credit reports for unusual activity. To that end, Nationwide offered a year of free credit monitoring and identity-fraud protection of up to \$1 million through a third-party vendor. Nationwide also suggested that Plaintiffs set up a fraud alert and place a security freeze on their credit reports. However, Nationwide's website explained that a security freeze could impede consumers' ability to obtain credit, and could cost a fee between \$5 and \$20 to both place and remove. Nationwide did not offer to pay for expenses associated with a security freeze.

Plaintiff Hancox filed a five-count putative class-action complaint against Nationwide in the United States District Court for the District of Kansas, and Plaintiff Galaria filed essentially the same complaint in the United States District Court for the Southern District of Ohio a month later. The Kansas district court transferred Hancox's action to the Ohio district court, which designated the dockets as related. In Counts I and II of the complaints, Plaintiffs allege that Nationwide willfully and negligently violated the Fair Credit Reporting Act (FCRA), Pub. L. No.

91-508, 84 Stat. 1114 (1970) (codified at 15 U.S.C. § 1681), by failing to adopt required procedures to protect against wrongful dissemination of Plaintiffs' data. In Counts III, IV, and V, Plaintiffs allege claims for negligence, invasion of privacy by public disclosure of private facts, and bailment, which also arose out of Nationwide's failure to secure Plaintiffs' data against a breach.

In support of their claims, Plaintiffs allege that there is an illicit international market for stolen data, which is used to obtain identification, government benefits, employment, housing, medical services, financial services, and credit and debit cards. Identity thieves may also use a victim's identity when arrested, resulting in warrants issued in the victim's name. According to the complaints, the Nationwide data breach created an "imminent, immediate and continuing increased risk" that Plaintiffs and other class members would be subject to this kind of identity fraud. R. 1, PID 3. Plaintiffs cite a study purporting to show that in 2011 recipients of data-breach notifications were 9.6 times more likely to experience identity fraud, and had a fraud incidence rate of 19%.

Plaintiffs allege that victims of identity theft and fraud will "typically spend hundreds of hours in personal time and hundreds of dollars in personal funds," incurring an average of \$354 in out-of-pocket expenses and \$1,513 in total economic loss. *Id.*, PID 13. To mitigate this risk, Plaintiffs "have suffered, and will continue to suffer" costs—both "financial and temporal"—that include "purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts." *Id.* The complaints seek damages for, among other things, the increased risk of fraud; expenses incurred in mitigating risk, including the cost of

credit freezes, insurance, monitoring, and other mitigation products; and time spent on mitigation efforts.

The district court granted Nationwide's motion to dismiss the complaints. First, the district court concluded that Plaintiffs did not have "statutory standing" under the FCRA and thus dismissed the FCRA claims for lack of subject-matter jurisdiction. R. 40, PID 408. Next, the district court addressed whether Plaintiffs had Article III standing to bring their negligence and bailment claims, concluded that Plaintiffs had not alleged a cognizable injury, and dismissed the claims for lack of jurisdiction. Lastly, the district court concluded that Plaintiffs had standing to bring their invasion-of-privacy claim but failed to state a claim for relief, and dismissed that claim with prejudice.

Plaintiffs moved for reconsideration and leave to amend, asserting that the district court erred in dismissing one of their FCRA claims. Plaintiffs did not seek reconsideration of the other four dismissed claims, which were omitted from the proposed amended complaint, but maintained their right to appeal the dismissals. Notably, the proposed amended complaint includes a new allegation that Plaintiff Galaria discovered three unauthorized attempts to open credit cards in his name. After checking with the credit-card companies, he learned that applications to open cards had been made using his name, Social Security number, and date of birth. The district court denied reconsideration and leave to amend, concluding that Plaintiffs had not demonstrated a clear error of law, and that the proposed amendment would not cure any deficiencies in the FCRA claim in any event.

Plaintiffs appeal the dismissal of their FCRA, negligence, and bailment claims for lack of jurisdiction, and the denial of their motions for reconsideration and leave to amend. Plaintiffs do not appeal the dismissal of their invasion-of-privacy claim.

II. Discussion

A. Article III standing

We review de novo the district court's determination of Article III standing. *McKay v. Federspiel*, 823 F.3d 862, 866 (6th Cir. 2016). "Article III of the Constitution limits the jurisdiction of federal courts to 'Cases' and 'Controversies,'" and "[t]he doctrine of standing gives meaning to these constitutional limits by 'identify[ing] those disputes which are appropriately resolved through the judicial process.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). The Supreme Court has explained that "the 'irreducible constitutional minimum' of standing consists of three elements." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (quoting *Lujan*, 504 U.S. at 560). A plaintiff "must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of a defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.*

The plaintiff "bears the burden of showing that he has standing," *Summers v. Earth Island Institute*, 555 U.S. 488, 493 (2009), and "[e]ach element of standing 'must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation.'" *Fair Elections Ohio v. Husted*, 770 F.3d 456, 459 (6th Cir. 2014) (quoting *Lujan*, 504 U.S. at 561). "Where, as here, a case is at the pleading stage, the plaintiff must 'clearly . . . allege facts demonstrating' each element." *Spokeo*, 136 S. Ct. at 1547 (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)). The court "must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Parsons v. U.S. Dep't of Justice*, 801 F.3d 701, 710 (6th Cir. 2015) (quoting *Warth*, 422 U.S. at 501).

Injury is “the ‘[f]irst and foremost’ of standing’s three elements.” *Spokeo*, 136 S. Ct. at 1547 (quoting *Steel Co. v. Citizens for Better Env’t*, 523 U.S. 83, 103 (1998)). “To establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560). Where plaintiffs seek to establish standing based on an imminent injury, the Supreme Court has explained “that ‘threatened injury must be *certainly impending* to constitute injury in fact,’ and that ‘[a]llegations of *possible* future injury’ are not sufficient.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (emphasis in original) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). However, the Supreme Court has also “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,” even where it is not “literally certain the harms they identify will come about.” *Id.* at 1150 n.5 (citing cases).

Here, Plaintiffs’ allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation. Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of “possible future injury” or “objectively reasonable likelihood” of injury that the Supreme Court has explained are insufficient. *Clapper*, 133 S. Ct. at 1147–48. There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year. Where a data

breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.

Thus, although it might not be “literally certain” that Plaintiffs' data will be misused, *id.* at 1150 n.5, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when Nationwide recommended taking these steps. And here, the complaints allege that Plaintiffs and the other putative class members must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts. Although Nationwide offered to provide some of these services for a limited time, Plaintiffs allege that the risk is continuing, and that they have also incurred costs to obtain protections—namely, credit freezes—that Nationwide recommended but did not cover. This is not a case where Plaintiffs seek to “manufacture standing by incurring costs in anticipation of non-imminent harm.” *Id.* at 1155. Rather, these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing.¹

This conclusion is in line with two recent decisions from the Seventh Circuit addressing standing in data-breach cases. In *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir.

¹The allegation in the proposed amended complaint that Plaintiff Galaria suffered three unauthorized attempts to open credit cards in his name further supports standing. However, Plaintiffs did not seek reconsideration of the district court's dismissal of their negligence and bailment claims for lack of Article III standing, and did not seek leave to amend the complaint for the purpose of bolstering the allegations in support of standing. The district court could not have abused its discretion in denying reconsideration and leave to amend for reasons that Plaintiffs expressly disclaimed. *See generally Leisure Caviar, LLC v. U.S. Fish & Wildlife Serv.*, 616 F.3d 612, 615–16 (6th Cir. 2010) (discussing the relevant standards). Regardless, we conclude that the allegations in the initial complaint are sufficient.

2015), the court held that victims of a data breach at a department store had established injury-in-fact by alleging a “substantial risk of harm” from the theft of their data. *Id.* at 693. The court explained: “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 a fraudulent charge or assume those consumers’ identities.” *Id.* The court reached the same conclusion in *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), where restaurant customers’ credit-card data was stolen in a data breach, because a “primary incentive” for a breach is to commit fraud. *Id.* at 965, 967.² The Ninth Circuit similarly found Article III standing in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), where employees brought suit after a thief stole a company laptop containing their personal information. *Id.* at 1141–43.

The Third Circuit reached a different conclusion in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). In *Reilly*, a hacker broke into a payroll processor’s network, but it was not clear “whether the hacker read, copied, or understood” the personal data stored on the system. *Id.* at 40, 44. The plaintiffs—whose data was in the system—alleged standing based on an increased risk of identity theft, but the court concluded that the injuries were too speculative because there would be an injury only “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.” *Id.* at 43. The Third Circuit also distinguished the case from data-breach cases where courts found standing: “Here, there is no evidence that the intrusion was intentional or malicious. . . . Indeed, no

²*Remijas* and *Lewert* both cite the Supreme Court’s decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), for the proposition that an “objectively reasonable likelihood” of injury is sufficient to support standing, *Lewert*, 819 F.3d at 966; *Remijas*, 794 F.3d at 693, but *Clapper* expressly rejects that standard. 133 S. Ct. at 1147. However, these references were not critical to the reasoning or outcome of either case.

identifiable taking occurred; all that is known is that a firewall was penetrated.” *Id.* at 44. Thus, *Reilly* is not on point where, as here, Plaintiffs allege an “identifiable taking”—the intentional theft of their data.³

Next, Plaintiffs’ injury must also be “‘fairly traceable’ to the conduct being challenged.” *Wittman v. Personhuballah*, 136 S. Ct. 1732, 1736 (2016) (quoting *Lujan*, 504 U.S. at 560–61). This element of standing “is not focused on whether the defendant ‘caused’ the plaintiff’s injury in the liability sense,” *Wuliger v. Mfrs. Life Ins. Co.*, 567 F.3d 787, 796 (6th Cir. 2009), because “causation to support standing is not synonymous with causation sufficient to support a claim.” *Parsons*, 801 F.3d at 715. Indeed, the Supreme Court has made clear that “[p]roximate causation is not a requirement of Article III standing.” *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1391 n.6 (2014). “To that end, the fact that an injury is indirect does not destroy standing as a matter of course.” *Parsons*, 701 F.3d at 713; *see also Warth*, 422 U.S. at 504. Rather, the traceability requirement mainly serves “to eliminate those cases in which a third party and not a party before the court causes the injury.” *Am. Canoe Ass’n v. City of Louisa Water & Sewer Comm’n*, 389 F.3d 536, 542 (6th Cir. 2004).

Here, Plaintiffs sufficiently allege that their injuries are fairly traceable to Nationwide’s conduct. For example, Plaintiffs allege that Defendants failed “to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff’s and other Class Members’ [data] to protect against anticipated threats to the security or integrity of such information.” R. 1, PID 11–12. Although hackers are

³To the extent *Reilly* suggests that more is required at the pleading stage, we find it unpersuasive. We must accept as true Plaintiffs’ allegations about the nature of the breach and the data stolen, and construe the complaints in Plaintiffs’ favor. *Parsons*, 801 F.3d at 710. These allegations might not be borne out by discovery, but are plausible, based on rational inferences from known facts, and are sufficient to survive a motion to dismiss.

the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because Nationwide allegedly failed to secure the sensitive personal information entrusted to its custody. In other words, but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data. These allegations meet the threshold for Article III traceability, which requires "more than speculative but less than but-for" causation. *Parsons*, 801 F.3d at 714.

This conclusion is consistent with the Eleventh Circuit's decision in *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012), which held that injuries from a data breach were fairly traceable to a defendant that failed to secure laptops that were then stolen. The Seventh and Ninth Circuit have also found the traceability requirement met in similar data-breach cases. *Lewert*, 819 F.3d at 969; *Remijas*, 794 F.3d at 696; *Krottner*, 628 F.3d at 1141. Further, in *Lambert v. Harman*, 517 F.3d 433, 438 (6th Cir. 2008), we held that identity theft was fairly traceable to a defendant that mishandled the plaintiff's personal data by releasing it online. True, the plaintiff in *Lambert* alleged conduct more egregious than the general allegations of inadequate security presented in Plaintiffs' complaints; but at the pleading stage, we "presume[] that general allegations embrace those specific facts that are necessary to support the claim." *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990).

Lastly, Plaintiffs must show that their injury "will likely be 'redressed' by a favorable decision." *Wittman*, 136 S. Ct. at 1736 (quoting *Lujan*, 504 U.S. at 560–61). Here, Plaintiffs seek compensatory damages for their injuries, and a favorable verdict would provide redress.

Thus, we conclude that Plaintiffs' complaints adequately allege Article III standing. Nationwide argues in the alternative that the dismissal of the negligence and bailment claims should nonetheless be affirmed on the basis that Plaintiffs failed to state claims for relief.

However, because the district court dismissed for lack of jurisdiction, we decline to grant a dismissal on the merits on appeal.

B. Statutory standing under the FCRA

We review de novo the district court's dismissal of Plaintiffs' FCRA claims for lack of subject-matter jurisdiction. *Askins v. Ohio Dep't of Agric.*, 809 F.3d 868, 872 (6th Cir. 2016). The district court concluded that the complaints allege a violation of the FCRA's statement of purpose rather than a substantive provision of the statute, and dismissed the FCRA claims for lack of statutory standing.

The Supreme Court has explained that the term "statutory standing" describes an inquiry into the question whether a plaintiff "falls within the class of plaintiffs whom Congress has authorized to sue" and therefore "has a cause of action under the statute." *Lexmark*, 134 S. Ct. at 1387–88 & n.4. However, this label is "misleading, since 'the absence of a valid (as opposed to arguable) cause of action does not implicate subject-matter jurisdiction, *i.e.*, the court's statutory or constitutional *power* to adjudicate the case.'" *Id.* (emphasis in original) (quoting *Verizon Md. Inc. v. Pub. Serv. Comm'n of Md.*, 535 U.S. 635, 642–43 (2002)); *see also* *Facione v. CHL Mortg. Trust 2006-J1*, 628 F. App'x 919, 920 (6th Cir. 2015) (noting the "confusion" caused by the term "statutory standing"). The question whether Plaintiffs have a cause of action is a merits issue that is "analytically distinct from the question whether a federal court has subject-matter jurisdiction." *Roberts v. Hamer*, 655 F.3d 578, 580 (6th Cir. 2011). If a plaintiff lacks statutory standing—in other words, does not have a cause of action—the proper course is to dismiss for failure to state a claim. *Id.* at 581.

Thus, the district court erred in concluding that it lacked subject-matter jurisdiction over the FCRA claims. As discussed, Plaintiffs have Article III standing to bring this action,⁴ and we see no other jurisdictional defect; the district court's contrary conclusion was based on an assessment of the merits. We go no further than reversing the district court's judgment as to its jurisdiction, and decline to address the merits issue on appeal. Instead, we return this question to the district court, which may dismiss for failure to state a claim if it concludes that Plaintiffs do not have a cause of action under the FCRA.

III. Conclusion

For these reasons, we **REVERSE** the dismissal of Plaintiffs' negligence, bailment, and FCRA claims for lack of subject-matter jurisdiction and **REMAND** for further proceedings.

⁴The Supreme Court has explained that FCRA claims may present Article III standing questions where the alleged FCRA violation is procedural in nature and the plaintiff suffers no harm. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). However, the district court did not address that question, and Plaintiffs have alleged an Article III injury in any event.

ALICE M. BATCHELDER, Circuit Judge, dissenting. I disagree with the majority’s conclusion that the complaints have adequately pled a causal connection between Nationwide’s alleged inaction and the plaintiffs’ alleged injury, which is necessary to establish Article III standing. As the plaintiffs have not satisfied this fundamental requirement of federal court jurisdiction, I would affirm the district court’s dismissal of their consolidated suit.

We need not take sides in the existing circuit split regarding whether an increased risk of identity theft is an Article III injury because, even assuming that it is, the plaintiffs have failed to demonstrate the second prong of Article III standing—causation. The causation element requires “a causal connection between the injury and the [defendant’s] conduct”—in other words, the injury must “be ‘fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.’” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (alterations omitted) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)). Intervening third party action generally defeats a plaintiff’s standing. *See, e.g., Binno v. Am. Bar Ass’n*, No. 12-2263, 2016 WL 3349212, at *3 (6th Cir. June 16, 2016) (rejecting a law school applicant’s constitutional standing to sue the ABA when his injury was actually caused by law school admissions offices and the administrators of the LSAT); *Ammex, Inc. v. United States*, 367 F.3d 530, 534 (6th Cir. 2004) (holding that a plaintiff could not sue the federal government to recover fuel taxes the government assessed on the plaintiff’s suppliers, because the suppliers had discretion to pass on the cost of the tax and “any alleged injury . . . was not occasioned by the Government”). If Galaria and Hancox suffered injury, it was at the hands of criminal third-party actors, and their complaints do not make the factual allegations necessary to fairly trace that injury to Nationwide.

At the motion-to-dismiss stage, the plaintiffs bear the same burden to plead the elements of Article III standing as they do to plead the elements of their cause of action. *See Lujan*, 504 U.S. at 561. Although “detailed factual allegations” are not required, the complaints must contain more than “‘naked assertions’ devoid of ‘further factual enhancement.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555, 557 (2007)); *see also White v. United States*, 601 F.3d 545, 552–53 (6th Cir. 2010) (applying *Iqbal* pleading requirements to allegations supporting Article III standing). The allegations must “nudge[]” the plaintiffs’ basis for standing “across the line from conceivable to plausible.” *Twombly*, 550 U.S. at 570.

Here, the complaints lack any factual link between Nationwide and the plaintiffs’ alleged injury. The complaints simply allege that hackers were in fact able to access the plaintiffs’ personal information. From that fact, the complaints conclude that Nationwide failed to protect that information. But plaintiffs make no factual allegations regarding how the hackers were able to breach Nationwide’s system, nor do they indicate what Nationwide might have done to prevent that breach but failed to do.¹ In short, there is no allegation of fact in either complaint that makes plausible the notion that Nationwide is at all responsible for the criminal acts that increased the plaintiffs’ risk of identity theft.

This case is distinguishable from those cases in which we have found Article III standing notwithstanding the intervening action of a third party. Nationwide’s alleged but unspecified

¹ The majority cites to paragraph 32 of the complaints, which alleges that Nationwide “flagrantly disregarded and/or violated [the plaintiffs’] privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of [the plaintiffs’ personal information and] to protect against anticipated threats to the security or integrity of such information.” This is a conclusory statement, not a factual allegation entitled to a presumption of truth. *See Iqbal*, 556 U.S. at 680–81.

negligence did not “motivate” the hacker’s criminal activity, *see Parsons v. U.S. Dep’t of Justice*, 801 F.3d 701, 714 (6th Cir. 2015), nor have the plaintiffs alleged any direct link between the hacker’s successful crime and an action of Nationwide, *Lambert v. Hartman*, 517 F.3d 433, 437–38 (6th Cir. 2008). Although a plaintiff need not prove that one particular actor out of many caused his harm, here the plaintiffs do not even allege wrongdoing by Nationwide that *might have* caused their harm. *See Am. Canoe Ass’n, Inc. v. City of Louisa Water & Sewer Comm’n*, 389 F.3d 536, 543 (6th Cir. 2004) (holding that a plaintiff could meet standing requirements at the pleading stage by alleging that the defendant was polluting and that the plaintiff was harmed by the pollution, even if other third-party actors were also polluting).

Lambert is particularly notable. A county clerk of court published Cynthia Lambert’s personal information on the internet by making public a traffic citation Lambert had received. 517 F.3d at 435. A criminal used this information to obtain a false driver’s license and make multiple purchases in Lambert’s name. *Id.* at 435. Lambert sued the clerk and the county for the violation of her privacy rights, but the defendants attacked her standing “on the basis that her injuries [were] not fairly traceable to the Clerk’s website.” *Id.* at 437. The court rejected this argument; although the defendants were not “the *direct* cause of Lambert’s injuries,” the plaintiff specifically linked the act of identity theft to the Clerk’s website through two factual allegations: (1) the driver’s license number on the traffic citation was incorrect by one digit, the same incorrect number on false driver’s license used to steal Lambert’s identity; and (2) the identity thief—who was caught—admitted obtaining the information from the website. *Id.* at 437–38.

Galaria and Hancox’s alleged injury is an increased risk of identity theft, not the theft itself as in *Lambert*. But they still need to allege facts establishing a causal link between that increased risk and something Nationwide did or did not do. Accusing Nationwide of “failing to

establish and/or implement appropriate . . . safeguards . . . to protect” customers’ personal information, without more, is insufficient to “allow[] the court to draw the reasonable inference” that the breach is fairly traceable to Nationwide. *Iqbal*, 556 U.S. at 678. It is just another way of saying that Nationwide didn’t prevent the data breach. But *no one* prevented the data breach; this hardly means that the plaintiffs have standing to sue the FBI or the Ohio Attorney General for not thwarting the hackers’ criminal activities. To establish standing, the plaintiffs must make some factual allegation of a *causal* connection. This they have failed to do.

The majority manufactures this causal connection on the plaintiffs’ behalf, stating that “but for Nationwide’s allegedly lax security, the hackers would not have been able to steal Plaintiffs’ data.” Nowhere does either complaint allege but-for causation. And although the majority is correct that but-for causation is not required for Article III standing, the plaintiffs’ allegations here are nothing more than sheer speculation. *See Parsons*, 801 F.3d at 714.

Other circuits’ contrary decisions in similar cases completely ignore the independent third party criminal action breaking the chain of causation. For example, the Eleventh Circuit held that plaintiffs satisfied the fairly traceable requirement by alleging only that the defendant “failed to secure [the plaintiffs’] information on company laptops, and that those laptops were subsequently stolen.”² *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012). And in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit overlooked the absence of any allegation that Neiman Marcus had specifically done anything that made the data breach easier or had failed to do anything that could have prevented it. 794 F.3d 688, 696 (7th Cir. 2015). The court did not explain how the risk of identity theft could be fairly traceable to Neiman Marcus when that risk was in fact the result of third party criminal action. *See also Lewert v. P.F.*

² Even this is more specific than what the plaintiffs have pled here.

Nos. 15-3386/3387, *Galaria et al. v. Nationwide Mutual Insurance Co.*

Chang's China Bistro, Inc., 819 F.3d 963, 969 (7th Cir. 2016) (ignoring the intervening third party action between the defendant hacked company and the plaintiffs' injury). We should not make this same mistake.

The majority sends the case back to the district court for analysis of Nationwide's motion to dismiss for failure to state a claim. Even were I to conclude that we have jurisdiction over this case, I do not believe a remand is necessary. The plaintiffs have not stated a claim for relief under the FCRA, because the complaint does not allege facts establishing that Nationwide is a "consumer reporting agency" or that Nationwide "furnished" a "consumer report" within the statutory definitions. *See, e.g., Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *3–4 (N.D. Ill. Jan. 21, 2015); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1286–87 (N.D. Ala. 2014); *see also Washington v. CSC Credit Servs. Inc.*, 199 F.3d 263, 265 (5th Cir. 2000) ("[T]he FCRA governs 'consumer reporting agencies' like Equifax and CSC [Credit Services] which maintain credit information on consumers and provide it to third parties."). And the plaintiffs have certainly not alleged the level of causation necessary to plead a claim of negligence. *See Whiting v. Ohio Dep't of Mental Health*, 750 N.E.2d 644, 647 (Ohio Ct. App. 2001) (quoting *Strother v. Hutchinson*, 423 N.E.2d 467, 470–71 (Ohio 1981)) ("'[P]roximate cause' is generally established 'where [a negligent] act . . . in a natural and continuous sequence, produces a result that would not have taken place without the act.'").

I respectfully dissent.