In the

United States Court of Appeals

For the Seventh Circuit

No. 17-2146

COMMUNITY BANK OF TRENTON, et al.,

Plaintiffs-Appellants,

v.

SCHNUCK MARKETS, INC.,

Defendant-Appellee.

Appeal from the United States District Court for the Southern District of Illinois.
No. 15-cv-1125 — **Michael J. Reagan**, *Chief Judge*.

ARGUED JANUARY 10, 2018 — DECIDED APRIL 11, 2018

Before WOOD, *Chief Judge*, HAMILTON, *Circuit Judge*, and BUCKLO, *District Judge*.*

HAMILTON, *Circuit Judge*. In late 2012, hackers infiltrated the computer networks at Schnuck Markets, a large Midwestern grocery store chain based in Missouri and known as "Schnucks." The hackers stole the data of about 2.4 million

* The Honorable Elaine E. Bucklo, United States District Judge for the Northern District of Illinois, sitting by designation.

credit and debit cards. By the time the intrusion was detected and the data breach was announced in March 2013, the financial losses from unauthorized purchases and cash withdrawals had reached into the millions. Litigation ensued.

Like many other recent cases around the country, this case involves a massive consumer data breach. See, e.g., *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). Unlike most other data-breach cases, however, the proposed class of plaintiffs in this case is comprised not of consumers but of financial institutions. Card-issuing banks and credit unions are required by federal law to indemnify their card-holding customers for losses from fraudulent activity, so our four plaintiff-appellant banks here bore the costs of reissuing cards and indemnifying the Schnucks hackers' fraud. See 15 U.S.C. § 1643(a) (limiting credit-card-holder liability for unauthorized use); 12 C.F.R. § 205.6 (limiting debit-card-holder liability for unauthorized use). The Article III standing and injury issues that arose in *Lewert*, *Remijas*, and many other data-breach cases with consumer plaintiffs are not issues in this case.

The principal issues in this case present fairly new variations on the economic loss rule in tort law. The central issue is whether Illinois or Missouri tort law offers a remedy to card-holders' banks against a retail merchant who suffered a data breach, above and beyond the remedies provided by the network of contracts that link merchants, card-processors, banks, and card brands to enable electronic card payments. The plaintiff banks assert claims under the common law as well as Illinois consumer protection statutes. Our role as a federal court applying state law is to predict how the states'

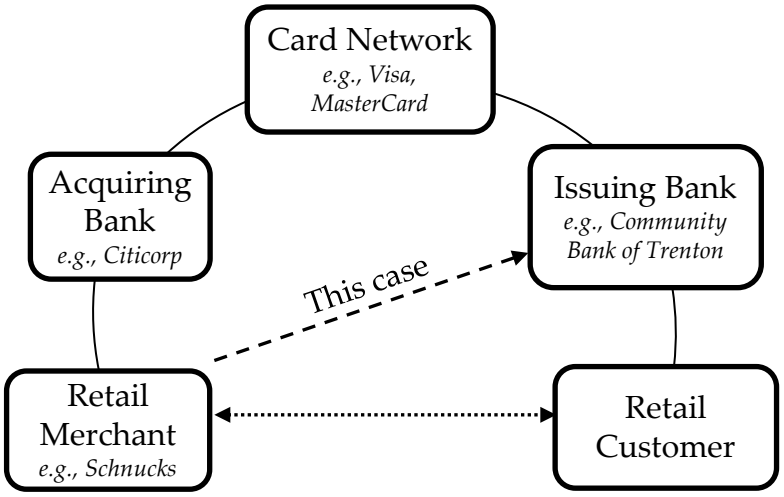
supreme courts would likely resolve these issues. We predict that both states would reject the plaintiff banks' search for a remedy beyond those established under the applicable networks of contracts. Accordingly, we affirm the district court's dismissal of the banks' complaint.

I. *Factual Background and Procedural History*

A. *Today's Electronic Payment Card System*

When a customer uses a credit or debit card at a retail store, the merchant collects the customer's information. This includes the card-holder's name and account number, the card's expiration date and security code, and, in the case of a debit card, the personal identification number. Collectively, this payment card information is known as "track data." At the time of purchase, the track data and the amount of the intended purchase are forwarded electronically to the merchant's bank (the "acquiring bank"), usually through a payment processing company. The acquiring bank then requests payment from the customer's bank (the "issuing bank") through the relevant card network—in this case, Visa or MasterCard. If the issuing bank approves the purchase, the transaction goes through within seconds. The customer's issuing bank then pays the merchant's acquiring bank the amount of the customer's purchase, which is credited to the merchant's account, minus processing fees. Contracts govern all of these relationships, although typically no contracts directly link the merchant (e.g., Schnucks) with the issuing banks (our four plaintiffs here). Here is a simplified diagram of this series of relationships:

The Card Payment System



In this case, Schnucks routed customer track data through a payment processor, First Data Merchant Services, to its acquiring bank, Citicorp. Citicorp then routed customer track data through the card networks to the issuing banks (plaintiffs here), who approved purchases and later collected payments from their customers, the card-holders. This web of contractual relationships facilitates the dotted line above: the familiar retail purchase by a customer from a merchant. Because Schnucks was the weak security link in this regime, the plaintiff banks seek to recover directly from Schnucks itself, a proposed line of liability represented by the dashed line above. This new form of liability would be in addition to the remedies already provided by the contracts governing the card payment systems.

B. *The Contracts that Enable the Card Payment System*

All parties in the card payment system agree to take on certain responsibilities and to subject themselves to specified contractual remedies. In joining the card payment system, issuing banks—including our plaintiffs here—agree to indemnify their customers in the event that a data breach anywhere in the network results in unauthorized transactions.[1] Visa requires issuers to "limit the Cardholder's liability to zero" when a customer timely notifies them of unauthorized transactions. Appellee App. at 99–100 (§ 4.1.13.3). MasterCard has the same requirement. *Id.* at 107 (§ 6.3).

For their parts, acquiring banks and their agents must abide by data security requirements. *Id.* at 102. As a merchant, Schnucks also agreed to abide by data security requirements in the contracts linking it to the card payment system. *Id.* at 54, 58, 70–72, 73. These data security rules are called the Payment Card Industry Data Security Standards or "PCI DSS." In their contracts, Schnucks, its bank, and its data processor effectively agreed to share resulting liabilities from any data breaches. *Id.* at 53–54, 70–71, 73 (Master Services Agreement §§ 4, 5.4; Bankcard Addendum §§ 23, 25, 28); see also *Schnuck Markets, Inc. v. First Data Merchant Services Corp.*, 852 F.3d 732, 735, 737–39 (8th Cir. 2017) ("*First Data*") (interpreting § 5.4 in light of this data breach at Schnucks). As we explain below, the specific details of these contractual

[1] This contractual duty goes beyond the federal law requirement to limit customer liability in the event of a data breach. See 15 U.S.C. § 1643(a); 12 C.F.R. § 205.6.

remedies do not matter here. What is important is that they exist at all, by agreements among the interested parties.

When a retailer or other party in the card payment system suffers a data breach, issuing banks must bear the cost, at least initially, of indemnifying their customers for unauthorized transactions and issuing new cards. The contracts that govern both the Visa and MasterCard networks then provide a cost recovery process that allows issuing banks to seek reimbursement for at least some of these losses. See Appellee App. at 102 (Visa), 110 (MasterCard). Schnucks agreed to follow card network "compliance requirements" for data security and to pay "fines" for noncompliance. *Id.* at 70. Our colleagues in the Eighth Circuit later read Schnucks' contract with its data processor and acquiring bank to include significant limits on Schnucks' share of the liability for losses of issuing banks. See *First Data*, 852 F.3d at 736, 737–39 (holding that contractual limit on liability favoring Schnucks applied to limit liabilities resulting from this data breach).[2]

---

[2] We can properly consider the remedies provided in the card brand rules and Schnucks' contractual agreements. A court deciding a motion to dismiss under Rule 12(b)(6) may consider documents that are attached to a complaint or that are central to the complaint, even if not physically attached to it. *Tierney v. Vahle*, 304 F.3d 734, 738 (7th Cir. 2002) (discussing Rules 12(b)(6) and 10(c)); see also, e.g., *Mueller v. Apple Leisure Corp.*, 880 F.3d 890, 895 (7th Cir. 2018) (affirming dismissal of contract claims); *Hecker v. Deere & Co.*, 556 F.3d 575, 578, 582–83 (7th Cir. 2009) (affirming dismissal of ERISA claims). Moreover, even the plaintiff banks say they want the court to consider these contracts "as to the liability issues" because they establish "the data protection and reporting standards to which Schnucks agreed to be bound." Reply Br. at 4. We cannot consider in isolation just those contractual provisions that plaintiffs find helpful. See *Minnesota Life Insurance Co. v. Kagan*, 724 F.3d 843, 850–51 (7th Cir. 2013). The substance of contracts among members of the card payment system is important in

C. *The Schnucks Data Breach and Response*

In early December 2012, hackers gained access to Schnucks' computer network in Missouri and installed malicious software (known as "malware") on its system. This malware harvested track data from the Schnucks system while payment transactions were being processed. As soon as payment cards were swiped at a Schnucks store and the unencrypted payment card information went from the card reader into the Schnucks system for payment, customer information was available for harvesting. The breach affected 79 of Schnucks' 100 stores in the Midwest, many of which are located in Missouri and Illinois, the states whose laws we consider here.

For the next four months, hackers harvested and sold customer track data, which were used to create counterfeit cards and to make unauthorized cash withdrawals, including from the plaintiff banks. Schnucks says it did not learn of the breach until March 14, 2013, when it heard from its card payment processor. A few days later, an outside consultant quickly identified the source of the problem. On March 30, Schnucks issued a press release announcing the data breach.

The plaintiff banks estimate that for every day the data breach continued, approximately 20,000 cards may have been

---

deciding whether to impose tort liability on top of existing contractual remedies. Cf. *Lone Star Nat'l Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421, 426 (5th Cir. 2013) (reversing dismissal of issuing banks' tort claims against payment processor; record was uncertain as to contractual remedies). From the contracts in our record, we know that the issuing banks (plaintiffs here), the specific acquiring bank (Citicorp), and the breached retail merchant (Schnucks) are all voluntarily part of the card payment systems and subject to their rules and remedies.

compromised. This means around 2.4 million cards in total were at risk from the Schnucks breach. Given this rate, plaintiffs estimate that more than 300,000 cards may have been compromised between March 14 and March 30, after Schnucks knew that security had been breached but before it announced that fact publicly. The plaintiff banks allege that numerous security steps could have prevented the breach and that those steps are required by the card network rules.[3] In fact, under the networks' contractual provisions, the card networks later assessed over $1.5 million in reimbursement charges and fees against Schnucks, which eventually split that liability with its card processor and acquiring bank. Brief for Appellants at 4, *First Data*, 852 F.3d 732 (8th Cir. 2017) (No. 15-3804), 2016 WL 284697, at *4; see also *First Data*, 852 F.3d at 735–36 (describing card networks' expectations, assessments, and resulting litigation).

D. *The Banks' Lawsuit*

The plaintiff banks, which may or may not have received some of those reimbursement funds, filed a lawsuit in 2014 seeking to be made whole directly by Schnucks. The banks dismissed their first complaint voluntarily and then filed this action in the Southern District of Illinois in October 2015. They amended their complaint in October 2016. The banks contend that despite the existence of the contractual remedies, issuing banks "cannot always recoup the reimbursed fraudulent charges" and must pay other fees and bear card reissuing

[3] These steps include installing appropriate antivirus software, complying with network segmentation and firewall standards, encrypting sensitive payment data, tracking and monitoring all access to payment information, and implementing two-factor authentication for remote access.

costs, which these banks seek to recover from Schnucks. Appellants' Br. at 11.[4]

In effect, the banks seek reimbursement for their losses above and beyond the remedies provided under the card network contracts. They say their losses include employee time to investigate and resolve fraud claims, payments to indemnify customers for fraudulent charges, and lost interest and transaction fees on account of changes in customer card usage. Plaintiffs estimate their damages in the tens of millions of dollars, placing this lawsuit in the same league as some others between financial institutions and breached retail merchants. See David L. Silverman, *Developments in Data Security Breach Liability*, 72 Bus. Law. 185, 185 (Winter 2016–17) (discussing three recent data breach cases settled by retail merchants for more than $15 million, including attorney fees).

In a thorough order, the district court dismissed all of the plaintiff banks' claims against Schnucks. No. 15-cv-01125-MJR, 2017 WL 1551330, at *1–2 (S.D. Ill. May 1, 2017). Jurisdiction was secure under the Class Action Fairness Act. The proposed plaintiff class of banks includes both Illinois and Missouri citizens; Schnucks is a citizen of Missouri; and

[4] The most important set of facts alleged by the plaintiffs involves the March 14–30 period, when Schnucks knew of the data breach but had not yet alerted banks and consumers. Because Schnucks "derives the majority of its revenue from electronic payment card transactions," plaintiffs believe Schnucks intentionally dragged its feet in announcing the data breach. See Am. Compl. ¶ 59. By having substandard security and by delaying disclosure of the breach, plaintiffs allege, Schnucks "saved the cost of implementing the proper payment card security policies, procedures, protocols, and hardware and software systems, and … wrongfully shifted the risk and expense of the Data Breach" to the banks. Am. Compl. ¶ 84.

the matter in controversy exceeds $5 million. See 28 U.S.C. § 1332(d)(2). The parties agreed that both Illinois and Missouri laws apply, given the proposed plaintiff class. None of the plaintiff banks' claims made it past the pleadings. The complaint was dismissed for failing to state a plausible claim under any of the banks' theories.

II. *Analysis*

A. *Standard of Review*

We review *de novo* the dismissal of a complaint for failure to state a claim under Rule 12(b)(6), accepting plaintiffs' factual allegations as true and drawing all permissible inferences in the plaintiffs' favor. *West Bend Mut. Insurance Co. v. Schumacher*, 844 F.3d 670, 675 (7th Cir. 2016). A plaintiff must, however, "provide more than mere labels and conclusions" and must go beyond "a formulaic recitation of the elements of a cause of action for her complaint to be considered adequate." *Id.*, quoting *Bell v. City of Chicago*, 835 F.3d 736, 738 (7th Cir. 2016). A party must also "proffer some legal basis to support his cause of action" and cannot expect either the district court or this court to "invent legal arguments" on his behalf. *County of McHenry v. Insurance Co. of the West*, 438 F.3d 813, 818 (7th Cir. 2006), quoting *Stransky v. Cummins Engine Co.*, 51 F.3d 1329, 1335 (7th Cir. 1995).

B. *Common Law Claims*

1. *Framing the Analysis*

The plaintiff banks' substantive claims all arise under state law, but the relevant state courts have not addressed the specific questions we face. Under *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938), our role in deciding these questions of state law is to predict how the highest courts of the respective states

would answer them. *In re Zimmer, NexGen Knee Implant Products Liability Litig.*, 884 F.3d 746, 751 (7th Cir. 2018); *Cannon v. Burge*, 752 F.3d 1079, 1091 (7th Cir. 2014). We are to take into account trends in a state's intermediate appellate decisions, see *In re Zimmer*, 884 F.3d at 751, but the focus is always a prediction about the state's highest court. See *Santa's Best Craft, LLC v. St. Paul Fire & Marine Insurance Co.*, 611 F.3d 339, 349 n.6 (7th Cir. 2010), citing *Taco Bell Corp. v. Continental Cas. Co.*, 388 F.3d 1069, 1077 (7th Cir. 2004) (concerned with making a "reliable prediction of how the Supreme Court of Illinois would rule"). In predicting state law in the relevant states, we try to avoid simply grafting abstract hornbook law principles onto the particular fact pattern in front of us, see *NLRB v. Int'l Measurement & Control Co.*, 978 F.2d 334, 339 (7th Cir. 1992) (refusing to defer to agency's prediction of state law based on "blackletter terms" without citing state court decisions), but we can look to well-reasoned decisions in other jurisdictions for guidance.

To frame the issues, we begin by examining the economic loss doctrine in commercial litigation. For more than fifty years, state courts have generally refused to recognize tort liabilities for purely economic losses inflicted by one business on another where those businesses have already ordered their duties, rights, and remedies by contract. The reason for this rule is that "liability for purely economic loss … is more appropriately determined by commercial rather than tort law," i.e., by the system of rights and remedies created by the parties themselves. *Indianapolis-Marion County Public Library v. Charlier Clark & Linard, P.C.*, 929 N.E.2d 722, 729 (Ind. 2010), citing *Miller v. U.S. Steel Corp.*, 902 F.2d 573, 574 (7th Cir. 1990) ("tort law is a superfluous and inapt tool for resolving purely commercial disputes" whose risks are better allocated by the

contracting parties themselves than by judges), and citing *Seely v. White Motor Co.*, 403 P.2d 145 (Cal. 1965). "The issue" in these cases "is not causation; it is duty," in the sense that tort law generally does not supply additional liabilities on top of specified contractual remedies. *Rardin v. T & D Machine Handling, Inc.*, 890 F.2d 24, 26, 27–28 (7th Cir. 1989) (applying Illinois law).

Courts invoking the economic loss rule trust the commercial parties interested in a particular activity to work out an efficient allocation of risks among themselves in their contracts. Courts "see no reason to intrude into the parties' allocation of the risk" when bargaining should be sufficient to protect the parties' interests, and where additional tort law remedies would act as something of a wild card to upset their expectations. *East River S.S. Corp. v. Transamerica Delaval Inc.*, 476 U.S. 858, 872–73, 875–76 (1986) (adopting economic loss rule in admiralty cases); see also *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 176 (3d Cir. 2008) (explaining *Robins Dry Dock & Repair Co. v. Flint*, 275 U.S. 303 (1927), an early case limiting tort liabilities for economic losses).

The doctrinal explanation is relatively simple: tort law often applies where there is "a sudden, calamitous accident as distinct from a mere failure to perform up to commercial expectations." *Rardin*, 890 F.2d at 29. In the latter case, contract law should be sufficient because a sophisticated business plaintiff could "have protected himself through his contractual arrangements" ahead of time. See *id.* at 28; see also *Chicago Heights Venture v. Dynamit Nobel of America, Inc.*, 782 F.2d 723, 729 (7th Cir. 1986) (applying Illinois law and comparing "the 'safety-insurance policy of tort law'" to the "'expectation-bargain protection policy' of contracts"); Mark

P. Gergen, *The Ambit of Negligence Liability for Pure Economic Loss*, 48 Ariz. L. Rev. 749, 752 (2006) (even when there is a need for tort liability, if conduct results in "solely pecuniary harm" and there are reasons to doubt tort law's efficacy in providing proper incentives, "the common law has erred on the side of preserving freedom of action, rather than on the side of protecting against harm").

This principle has also been applied in other contexts. For example, when physical or personal injuries occur because of defective products, "[s]ociety has a great interest in spreading the cost of such injuries," but when a product causes economic loss by simply failing to perform as expected, tort liability is unwarranted; the Uniform Commercial Code already provides "a finely tuned mechanism for dealing with the rights of parties to a sales transaction with respect to economic losses." *Sanco, Inc. v. Ford Motor Co.*, 579 F. Supp. 893, 897, 898 (S.D. Ind. 1984) (Dillin, J.), citing *Seely*, 403 P.2d at 151. Similarly, in construction disputes, where the complex relationship of contractors and subcontractors is analogous to the web of contracts in this case, the economic loss rule encourages contracting parties to "prospectively allocate risk and identify remedies within their agreements." *Flagstaff Affordable Housing Ltd. Partnership v. Design Alliance, Inc.*, 223 P.3d 664, 670 (Ariz. 2010). "These goals would be undermined by an approach that allowed extra-contractual recovery for economic loss based not on the agreement itself, but instead on a court's post hoc determination that a construction defect"—or a data breach—"posed risks of other loss … ." *Id.*

Some form of the economic loss rule is the rule in most jurisdictions in the United States, *Rardin*, 890 F.2d at 28,

including Illinois and Missouri. In Illinois, it is known as the *Moorman* doctrine, from *Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443 (Ill. 1982). Illinois applies *Moorman* to services as well as the sale of goods because both business contexts provide "the ability to comprehensively define a relationship" by contract. *Fireman's Fund Ins. Co. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1200 (Ill. 1997), quoting *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co.*, 636 N.E.2d 503, 514 (Ill. 1994). Illinois recognizes three exceptions, but none applies here: for personal injuries or property damage resulting from sudden or dangerous occurrences, for fraud, and for negligent misrepresentations by professional business advisors. *Id.* at 1199. Missouri more generally prohibits "a plaintiff from seeking to recover in tort for economic losses that are contractual in nature." *Autry Morlan Chevrolet Cadillac, Inc. v. RJF Agencies, Inc.*, 332 S.W.3d 184, 192 (Mo. App. 2010), citing *Crowder v. Vandendeale*, 564 S.W.2d 879, 881 (Mo. 1978). Exceptions to the Missouri economic loss doctrine are limited to losses arising from personal injuries, property damage or destruction, or from special relationships giving rise to fiduciary duties. *Autry Morlan Chevrolet*, 332 S.W.3d at 192, 194.

The parties offer numerous doctrinal arguments about the economic loss rule and common law duties. Before we dig into those arguments, we pause to explain the broader choice between paradigms in this case. In deciding whether economic losses are recoverable in tort law, courts face a choice between what scholars have called the "stranger paradigm" and the "contracting parties paradigm." Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DePaul L. Rev. 339, 344 (2017); see also Dan B. Dobbs, *An Introduction to Non-Statutory Economic Loss Claims*, 48 Ariz.

L. Rev. 713, 714 (2006); William Powers, Jr., *Border Wars*, 72 Tex. L. Rev. 1209, 1229 (1994) (addressing more general issue of borders between contract and tort law in terms of competing paradigms); Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 Wash. & Lee L. Rev. 523, 546 (2009) (addressing purposes of rule).

The stranger paradigm fits "when an actor's negligence causes financial losses to a party with whom the actor has no pre-existing relationship." Sharkey, 66 DePaul L. Rev. at 344. The stranger paradigm seeks to set the "parameters of the duty of reasonable care … at physical injuries and property damage" and, traditionally, does not allow recovery for simple economic losses. *Id.* But some courts taking this approach in data breach cases have decided to allow tort recovery anyway, both for consumers and for sophisticated financial institutions. These courts, one scholar argues, "are doing so not only in an ad hoc manner, but also by stretching and misapplying the stranger paradigm" instead of taking a "broader regulatory perspective." *Id.* at 383.

The contracting parties paradigm approaches the problem differently. Under this paradigm, "the question is whether a duty should be imposed *by* [tort] *law* … over and above … any voluntary allocation of risks and responsibilities already made between the contracting parties." *Id.* at 344–45. In this approach, the presence of contract remedies sets a boundary for tort law. If "contract law purports to decide the case, the negligence paradigm … should stay in the background." *Id.* at 345 n.16, quoting Powers, 72 Tex. L. Rev. at 1229 (alteration in original).

Courts using the contracting parties paradigm first take into account the mechanisms the parties have chosen to

allocate the risks they face. Courts then consider whether these mechanisms have sufficiently reduced the externalities visited upon third parties, or whether the breached entities need additional financial incentives to pursue better data security. *Id.* at 382–83. The ultimate question is whether these arrangements already place costs on "the cheapest cost avoider" or whether additional tort liability is necessary because the existing contracts "externalize significant risk onto hapless third parties." *Id.* at 383.

The plaintiff banks emphasize here that they have no direct contractual relationship with Schnucks. That's true, but it does not undermine use of the contracting parties paradigm. The plaintiff banks and Schnucks all participate in a network of contracts that tie together all the participants in the card payment system. That network of contracts imposes the duties plaintiffs rely upon and provides contractual remedies for breaches of those duties. See *Annett Holdings, Inc. v. Kum & Go, L.C.*, 801 N.W.2d 499, 504 (Iowa 2011) ("When parties enter into a chain of contracts, even if the two parties at issue have not actually entered into an agreement with each other, courts have applied the 'contractual economic loss rule' to bar tort claims for economic loss, on the theory that tort law should not supplant a consensual network of contracts."), citing Dobbs, 48 Ariz. L. Rev. at 726 (discussing relationships among buyers, retailers, and manufacturers and landowners, contractors, and subcontractors). Under these circumstances, we believe the Illinois and Missouri courts would most likely use the contracting parties paradigm.

As described above, in deciding to join the card payment system, Schnucks agreed to abide by the data security standards of the industry, the PCI DSS. Schnucks also agreed

to be subject to assessments and fines from the card networks in the event that it was responsible for data breaches and unauthorized card activity. On their end, the plaintiff banks agreed to exceed federal requirements for indemnifying their card-holders and also consented to the remedial assessment and reimbursement process provisions and related risks.

Even if these issuing banks had heard of this particular merchant before its data breach was announced, parties to the card payment system are not ships passing (or colliding) in the night. All parties involved in the complicated network of contracts that establish the card payment system have voluntarily decided to participate and to accept responsibility for the risks inherent in their participation. This includes at least some risk of not being fully reimbursed for the costs of another party's mistake.

The details of these reimbursement remedies are not fully apparent from the contract excerpts presented in this case. But what matters is not the details of the remedies but their *existence*. Merchants and acquiring banks face the financial cost of data breaches through the card networks' reimbursement regime. That means the cheapest cost avoiders (the data handlers) already bear the cost of data security protocols and breaches. The plaintiff banks in this case make no effort to explain how this system is inadequate in providing reimbursement. They ask us, though, to predict the recognition of new theories of state tort liability through simplistic application of sweeping black-letter tort law principles, leaving the card network reimbursement systems to be considered as mere damage issues on remand.

Given this network of contracts and contractual remedies, we decline plaintiffs' invitation to apply a version of the

stranger paradigm. We doubt the wisdom of recognizing new, supplemental liabilities without a clear sense of why they are necessary. It's not as if the banks have no rights or remedies at all. This is also not a situation where sensitive data is collected and then disclosed by private, third-party actors who are not involved in the customers' or banks' direct transactions. See, e.g., *In re Equifax, Inc., Customer Security Data Breach Litigation*, — F. Supp. 3d —, 2017 WL 6031680 (J.P.M.L. 2017). The plaintiff banks seek additional recovery because they are disappointed by the reimbursement they received through the contractual card payment systems they joined voluntarily.

The legal issues raised by the plaintiff banks are similar to the issues that arise in large construction projects with layers of contractors, subcontractors, sub-subcontractors, and so on. There may be no direct contractual relationship between a negligent subcontractor and other businesses that suffer from delays and expenses it caused. Yet all participants are tied into a network of contracts that allocate the risks of sub-standard or slow work. In such cases, as the Indiana Supreme Court has explained, claims of purely economic loss are better treated under contract law, without supplementary remedies from tort law. See *Indianapolis-Marion County Public Library*, 929 N.E.2d at 740 ("the substance of our holding is that when it comes to claims for pure economic loss, the participants in a major construction project define for themselves their respective risks, duties, and remedies in the network or chain of contracts governing the project"). Illinois and Missouri have reached the same general conclusion about contractual relationships in construction disputes. See *Fireman's Fund Insurance Co.*, 679 N.E.2d at 1198, 1201–02 (holding that economic loss rule barred bar tort recovery by subcontractor's insurance company against construction engineers); *Fleischer*

v. Hellmuth, Obata & Kassabaum, Inc., 870 S.W.2d 832, 834, 837 (Mo. App. 1993) (holding that in absence of direct contract, architect owed no duty of care and was not liable to construction manager in tort for economic losses as result of negligent performance of contract with property owner).

As we explain in more detail below, we do not see either a paradigmatic or doctrinal reason why either Illinois or Missouri would recognize a tort claim by the issuing banks in this case, where the claimed conduct and losses are subject to these networks of contracts. We now turn to plaintiffs' more specific doctrinal arguments.

2. *Negligence Claims*

a. Illinois Law

Plaintiffs allege that Schnucks, a retail merchant, had a common law duty to safeguard customers' track data and that the duty extends to its customers' banks. We first consider this question under Illinois tort law, which asks whether the defendant had "an obligation of reasonable conduct for the benefit of the plaintiff" using a four-factor analysis. *Marshall v. Burger King Corp.*, 856 N.E.2d 1048, 1057 (Ill. 2006). Though duty is a basic concept in tort law, the Illinois Supreme Court has not directly spoken to this question in the context of data breaches, so "we consider decisions of intermediate appellate courts unless there is good reason to doubt the state's highest court would agree with them." *Anicich v. Home Depot U.S.A., Inc.*, 852 F.3d 643, 649 (7th Cir. 2017), citing *Rodas v. Seidlin*, 656 F.3d 610, 626 (7th Cir. 2011).

The Illinois Appellate Court addressed this topic in *Cooney v. Chicago Public Schools*, where Social Security numbers and other personal information of more than 1,700 former school

employees were disclosed in a mailing. 943 N.E.2d 23, 27 (Ill. App. 2010). The *Cooney* court first considered whether a duty to safeguard personal information was imposed by federal or state statutes. It rejected the theory that the Illinois Personal Information Protection Act (PIPA) or the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposed any such duty beyond providing notice of a security breach. *Id.* at 28.

Cooney then rejected "'a new common law duty' to safeguard information," writing that "we do not believe that the creation of a new legal duty beyond legislative requirements,"—i.e., beyond notice—"is part of our role on appellate review." *Id.* at 28–29. The *Cooney* court concluded that "the legislature has specifically addressed the issue and only required the [School] Board to provide notice of the disclosure," which it had done. *Id.* at 29. The contractor who actually sent the offending mailing, All Printing & Graphics, Inc., was similarly excused from tort liability for its negligence. *Id. Cooney* did not characterize its holding on the duty question as an application of the economic loss rule. The opinion reads as a more general statement that no duty to safeguard personal information existed, regardless of the kind of loss. See *id.* at 28–29. Nothing in the *Cooney* analysis indicates that retail merchants like Schnucks should or would be treated differently than the former employer and contractor at issue there. In the absence of some other reason why the Illinois Supreme Court would likely disagree with the *Cooney* analysis on this issue of duty under the common law, see *Anicich*, 852 F.3d at 649, we predict that the state court

would not impose the common law data security duty the plaintiff banks call for here.[5]

Even if *Cooney* had not come to this conclusion, Illinois would probably apply the economic loss rule to bar recovery anyway. As mentioned above, Illinois' *Moorman* doctrine has three exceptions, *Fireman's Fund Insurance Co.*, 679 N.E.2d at 1199–1200, but none applies here. There was no sudden or dangerous occurrence. Data breaches are a foreseeable (and foreseen) risk of participating in the card networks, not an unexpected physical hazard. See *Moorman*, 435 N.E.2d at 449, citing *Cloud v. Kit Mfg. Co.*, 563 P.2d 248, 251 (Alaska 1977) (severe property damage caused by fire). Though the plaintiff banks suggested in their complaint that Schnucks engaged in "wrongful conduct" or "wrongful actions … [and] omissions" by not immediately announcing the data breach, see Am. Compl. ¶¶ 59, 112-13, 117-18, these allegations fail to identify specifically an actionable fraudulent statement under Illinois law. See below at 33–36; see also *Moorman*, 435 N.E.2d at 452, citing *Soules v. General Motors Corp.*, 402 N.E.2d 599, 601 (Ill. 1980) (involving allegations of falsified franchisee financial reports). Finally, Schnucks did not have a professional advisory relationship with the plaintiff banks here, so that exception also does not apply. See *Moorman*, 435 N.E.2d at 452, citing *Rozny v. Marnul*, 250 N.E.2d 656, 663 (Ill.

[5] The plaintiff banks attempt to distinguish *Cooney* by pointing out that track data, as opposed to Social Security numbers, can be used more easily to cause lasting financial harm. From the card-holding consumer's perspective, given federally-mandated and card network-promised indemnification, this may or may not be true. And the plaintiffs point to no Illinois authority that explains why this difference, or the fact that financial institutions seek to impose this duty here, should change the result.

1969) (permitting recovery for economic losses caused by "a surveyor's professional mistakes"); see also *In re Michaels Stores Pin Pad Litigation*, 830 F. Supp. 2d 518, 530 (N.D. Ill. 2011) (explaining *Fireman's Fund* and other Illinois "professional malpractice" cases).

The plaintiff banks respond to these points by claiming that Illinois' economic loss rule does not apply when the duty is "extra-contractual." The banks claim that a duty attaches because there is no direct contract between these parties. The problem is that all parties in the card networks (including card-holding customers) expect everyone to comply with industry-standard data security policies *as a matter of contractual obligation*. See above at 5–6. *Cooney* shows that Illinois has not recognized an independent common law duty to safeguard personal information. The banks' argument also fails to account for the scope of the *Moorman* doctrine. Schnucks assumed contractual data security responsibilities in joining the card networks. Even if the plaintiff banks were not direct parties to agreements with Schnucks, they seek additional recovery for the breach of those contractual duties. "Even in the absence of an alternative remedy in contract," Illinois does not permit tort recovery for businesses who seek to correct the purely economic "defeated expectations of a commercial bargain." *2314 Lincoln Park West Condo. Ass'n v. Mann, Gin, Ebel & Frazier, Ltd.*, 555 N.E.2d 346, 350 (Ill. 1990), quoting *Anderson Elec., Inc. v. Ledbetter Erection Corp.*, 503 N.E.2d 246, 249 (Ill. 1986). The plaintiff banks are disappointed in the amounts the card networks' contractual reimbursement process provided. That type of tort claim is not permitted under *Moorman*.

b. Missouri Law

The Missouri appellate courts have said less than Illinois appellate courts on this question of duty. All the same elements important to the *Cooney* court, though, are also present in Missouri law. The Missouri courts use the same four-factor common law duty test. Compare *Hoffman v. Union Elec. Co.*, 176 S.W.3d 706, 708 (Mo. 2005), with *Marshall*, 856 N.E.2d at 1057. Missouri, like Illinois, has a data privacy statute whose only consumer-facing mandate is notice. Compare Mo. Ann. Stat. § 407.1500 (2017), with 815 Ill. Comp. Stat. 530/10 (2017); see also Sharkey, 66 DePaul L. Rev. at 340 n.2 (noting that 47 states have notice statutes and that only three states "take statutory protection a step further"). In addition, the state's attorney general has "exclusive authority" for enforcing Missouri's data breach notice statute by a civil action. § 407.1500(4) (2017).[6]

Other state legislatures have acted to impose the kind of reimbursement or damages liability the plaintiff banks call for here. Minnesota, Nevada, and Washington stand out as examples. See Minn. Stat. Ann. § 325E.64, subd. 3 (2017) (requiring reimbursement and imposing liability); Nev. Rev. Stat. Ann. § 603A.215(1), (3) (2017) (requiring PCI DSS compliance, but holding harmless compliant data collectors who are less than grossly negligent); Wash. Rev. Code Ann. § 19.255.020(3) (2017) (requiring reimbursement). We think the Missouri courts would take notice of these state laws and

[6] So far, only one court has examined this statute in a data breach case in a reported opinion. It predicted that no such negligence cause of action exists under Missouri law. *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009).

draw the inference that the Missouri legislature has chosen not to go as far. There may be statutes in other states that envision some type of monetary recovery, see *Amburgy*, 671 F. Supp. 2d at 1056, though it is clear that Missouri is not one of them. See § 407.1500; see also Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 Ariz. L. Rev. 1171, 1185–87 (2014).

Even if Missouri courts were not convinced by these comparisons and recognized a common law duty to safeguard customer data, the economic loss doctrine would still thwart the plaintiff banks' claims. Missouri does not permit "recovery in tort for pure economic damages" without personal injuries or property damage. *Autry Morlan Chevrolet Cadillac, Inc. v. RJF Agencies, Inc.*, 332 S.W.3d 184, 192 (Mo. App. 2010). Missouri's economic loss doctrine applies to "losses that are contractual in nature," *Captiva Lake Investments, LLC v. Ameristructure, Inc.*, 436 S.W.3d 619, 628 (Mo. App. 2014), citing *Autry Morlan Chevrolet*, 332 S.W.3d at 192, which, as explained above regarding the contracting parties paradigm, applies here. There is an exception from the economic loss rule for special relationships that give rise to a fiduciary duty, but "the existence of a business relationship does not give rise to a fiduciary relationship, nor a presumption of such a relationship" short of, for example, a "financial partnership" or principal-agent relationship. See *Autry Morlan Chevrolet*, 332 S.W.3d at 194, 195 (citations omitted). Like Illinois, Missouri is not likely to recognize the negligence claims the plaintiff banks assert here.

3. *Negligence Per Se*

The plaintiff banks' negligence *per se* claims fail because of the same statutory inferences. Neither Illinois nor Missouri

has legislatively imposed liability for personal data breaches, opting instead to limit their statutory intervention to notice requirements. *Cooney*, 943 N.E.2d at 28–29; *Amburgy*, 671 F. Supp. 2d at 1055. This is critical. Both states require a plaintiff to show, as the first element of a negligence *per se* action, that a statute or ordinance has been violated. Departures from industry custom are not sufficient, since industry custom would be a source of common law duties to be litigated in a negligence action. See *Bier v. Leanna Lakeside Property Ass'n*, 711 N.E.2d 773, 783 (Ill. App. 1999); *Sill v. Burlington Northern Railroad*, 87 S.W.3d 386, 392 (Mo. App. 2002).[7]

To bolster their negligence and negligence *per se* arguments, the plaintiff banks cite two district court cases declining to dismiss similar claims by banks against retail merchants. These cases are not persuasive regarding the common law of Illinois or Missouri. One case consciously sought to further statutory data security breach policies not present here. *In re Target Corp. Customer Data Security Breach Litig.*, 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014) (denying in

[7] Plaintiffs allege a violation of the Federal Trade Commission Act, 15 U.S.C. § 45, but they do not point to any FTC interpretations or court interpretations that extend its coverage to financial institutions in merchant data breach cases. *Irwin v. Jimmy John's Franchise, LLC* and *FTC v. Wyndham Worldwide Corp.* both involved customer injuries, not actions by their banks. 175 F. Supp. 3d 1064 (C.D. Ill. 2016); 799 F.3d 236 (3d Cir. 2015). The Illinois Consumer Fraud and Deceptive Business Practices Act incorporates by reference Commission and court interpretations of the FTCA, 815 Ill. Comp. Stat. 505/2, but again, plaintiffs point us to no such interpretations that support their claim of an FTCA violation here. These FTCA arguments are too underdeveloped to consider further. See *Bonte v. U.S. Bank, N.A.*, 624 F.3d 461, 465–67 (7th Cir. 2010) (affirming motion to dismiss generalized claim when appellants "provided precious little in the way of argument" in either district court or appeal).

part motion to dismiss). The other was based on a prediction of Georgia law that seems to have been incorrect. *In re The Home Depot, Inc., Customer Data Security Breach Litig.*, No. 1:14-md-2583-TWT (MDL No. 2583), 2016 WL 2897520, at *6–7 (N.D. Ga. May 18, 2016) (same).[8] The district court here was correct not to follow these cases on this point.

4. *Other Common Law Claims*

The plaintiff banks assert three other claims sounding in the common law of contracts: unjust enrichment, implied contract, and third-party beneficiary. The district court correctly dismissed them as well. All three fail because of basic contract law principles.

Illinois law and Missouri law on these common law contract theories are similar. Both refuse to recognize unjust enrichment claims where contracts already establish rights and remedies. *Guinn v. Hoskins Chevrolet*, 836 N.E.2d 681, 704 (Ill. App. 2005) ("where there is a specific contract that governs the relationship of the parties, the doctrine of unjust enrichment has no application" (brackets and citation omitted)); *Howard v. Turnbull*, 316 S.W.3d 431, 438 (Mo. App. 2010) ("plaintiff's entering into an agreement with known risks precluded recovery under an unjust enrichment claim when an anticipated contingency occurred"), citing *Farmers New World Life Ins. Co. v. Jolley*, 747 S.W.2d 704, 707 (Mo. App. 1988).

[8] The Court of Appeals of Georgia later disagreed with the *Home Depot* prediction of state law. *McConnell v. Dep't of Labor*, 787 S.E.2d 794, 797 n.4 (Ga. App. 2016), *vacated on other grounds*, *McConnell v. Dep't of Labor*, 805 S.E.2d 79 (Ga. 2017).

Illinois and Missouri also do not recognize implied contracts where written agreements define the business relationship. *Industrial Lift Truck Service Corp. v. Mitsubishi Int'l Corp.*, 432 N.E.2d 999, 1002 (Ill. App. 1982) ("Quasi-contract is not a means for shifting a risk one has assumed under contract."); *City of Cape Girardeau ex rel. Kluesner Concreters v. Jokerst, Inc.*, 402 S.W.3d 115, 121–22, 122 (Mo. App. 2013) (contract may be implied by law where "there is no formal contract" covering specific subject of dispute).

Neither state recognizes third-party beneficiary claims unless the beneficiary is identified or the third-party benefit is clearly intended by the contracting parties. Construction law is again helpful here. Illinois and Missouri have required a subcontractor to show that the contract in question between the principal parties clearly extends the rights of a third-party beneficiary. See *L.K. Comstock & Co. v. Morse/UBM Joint Venture*, 505 N.E.2d 1253, 1257 (Ill. App. 1987); *Drury Co. v. Missouri United School Insurance Counsel*, 455 S.W.3d 30, 34–35 (Mo. App. 2014).

As the district court found, Schnucks was not unjustly enriched. Its card-paying customers paid the same amount as those paying in cash; thus there is no unjust enrichment left uncovered outside of the card payment system contracts. As for an implied contract, the First Circuit has recognized an implied contract between a grocery store's *customers* and the store over the safeguarding of personal data. See *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 158–59 (1st Cir. 2011) (predicting Maine law). In this case, however, the only business activity between the plaintiff banks and Schnucks happened (nearly instantaneously) through the indirect route of the card payment system, not in a direct face-to-face retail

transaction. Even if we assume that Illinois or Missouri would accept the *Hannaford Brothers* logic, in the absence of any state authority on the point, we see no basis to predict that either state would extend that logic to find that the implied contractual duty extended to a customer's bank.

Similarly, we have no reason to think Illinois or Missouri would conclude that a retail merchant and its customer specifically intended the customer's bank to be a third-party beneficiary of their retail transaction. Illinois has rejected this theory where a construction subcontractor (not unlike the plaintiff banks here) sought damages for a breach of the contract between a construction manager and a construction client (like the retail merchant and customer here, respectively), where provisions of the contract were inconsistent with the idea that it envisioned the subcontractor as a third-party beneficiary. *L.K. Comstock & Co.*, 505 N.E.2d at 1257. Missouri has permitted third-party recovery in the context of a subcontractor and a construction client's insurance policy, though apparently only because the relevant contract specifically named "the Owner, the Contractor, *Subcontractors* and Sub-subcontractors in the Project" in its insurance provisions. *Drury Co.*, 455 S.W.3d at 35 (emphasis added).

The plaintiff banks have not argued on appeal that the card payment system contracts specifically envision them as a third-party beneficiary regarding the data security provisions, nor did they argue this point in the district court beyond vague references to the interchange fees the issuing banks receive simply for being part of the card payment system. See Dkt. 65 at 17; Am. Compl. ¶ 24. This is not enough to overcome the "strong presumption" in Illinois law "that

parties intend a contract to apply solely to themselves" for enforcement purposes. *Bank of America, N.A. v. Bassman FBT, L.L.C.*, 981 N.E.2d 1, 11 (Ill. App. 2012); see also *Martis v. Grinnell Mut. Reinsurance Co.*, 905 N.E.2d 920, 924 (Ill. App. 2009) ("It must appear from the language of the contract that the contract was made for the direct, not merely incidental, benefit of the third person."); accord, *FDIC v. G. III Investments, Ltd.*, 761 S.W.2d 201, 204 (Mo. App. 1988) ("The party claiming rights as a third party beneficiary has the burden of showing that provisions in the contract were intended to be made for his direct benefit.").

No express contract exists between Schnucks and its customers (beyond the basic exchange of products for payment), let alone one that specifically intends to include the plaintiff banks as third-party beneficiaries. As with construction contracts, the direct rights and reimbursement possibilities provided by the web of contracts, either for the construction job or the card payment system, define the limits of recovery. See, e.g., *Indianapolis-Marion County Public Library v. Charlier Clark & Linard, P.C.*, 929 N.E.2d 722, 740 (Ind. 2010). In this case, the web of contracts also precludes resort to secondary common law contract theories. We affirm the district court's rejection of these theories.

5. *Decisions in Other Circuits*

One other federal circuit court has reached a different prediction of state law on facts similar to these. Our colleagues in the Fifth Circuit predicted that New Jersey would recognize a negligence claim brought by an issuing bank against a payment processor, though not retail merchants. See *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013). Our conclusion is

different for at least two reasons. First, the *Lone Star* court relied on New Jersey's practice of being "a leader in expanding tort liability." *Id.* at 426–27, quoting *Hakimoglu v. Trump Taj Mahal Assocs.*, 70 F.3d 291, 295 (3d Cir. 1995) (Becker, J., dissenting). Second, unlike the *Lone Star* court, we know enough about the card network agreements in our record for them to inform our analysis. See 729 F.3d at 426.

Our predictions here are closer to the analysis in two cases from the Third and First Circuits. The Third Circuit applied the economic loss rule to bar negligence claims and rejected most of the other theories invoked by issuing banks against a breached retail merchant. *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175–78, 179–83 (3d Cir. 2008). Though the *Sovereign Bank* court reached a different conclusion about the third-party beneficiary claims in that case, *id.* at 168–73, here we have no specific argument on appeal to support the plaintiff banks' claims for third-party beneficiary status.

Similarly, the First Circuit has rejected a negligence theory because of the economic loss rule and also rejected a third-party beneficiary theory under the card payment system contracts. *In re TJX Companies Retail Security Breach Litig.*, 564 F.3d 489, 498–99 (1st Cir. 2009). In that case, a negligent misrepresentation claim survived "on life support," in light of the fact that the Massachusetts courts had recently handled a similar case that way. See *id.* at 494–96. Here we are presented with no such state authority on a negligent misrepresentation theory.

C. *Illinois Statutory Claims – The ICFA*

1. *The Plaintiff Banks' Claims*

We turn next to plaintiffs' claims under Illinois statutes. (As noted, Missouri provides no statutory cause of action for financial institutions in retail data breaches.) The plaintiff banks allege that Schnucks violated the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA) by engaging in an unfair practice of having poor data security procedures. See 815 Ill. Comp. Stat. 505/2, 505/10a. The banks also allege that Schnucks violated the Illinois Personal Information Protection Act (PIPA), 815 Ill. Comp. Stat. 530/10, and point out that PIPA violations are identified by statute as *per se* unlawful practices actionable under the ICFA, 815 Ill. Comp. Stat. 530/20. We affirm the district court's rejection of both theories in this case.

2. *Basic Elements of an ICFA Claim*

We first explain the relevant features of the ICFA before explaining why this claim fails as a matter of law. A plaintiff bringing a private claim under the ICFA must show five elements, the first of which is "a deceptive act or practice by the defendant." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 849–50 (Ill. 2005). Because the statute's right of action is available to "Any person who suffers actual damage as a result of a violation," *id.*, quoting 815 Ill. Comp. Stat. 505/10a(a), Illinois courts have interpreted the ICFA to apply not only in consumer-against-business cases but also in some cases when "both parties to the transaction are business entities." *Law Offices of William J. Stogsdill v. Cragin Fed. Bank for Savings*, 645 N.E.2d 564, 566–67 (Ill. App. 1995). A mere breach of contract, though, "does not amount to a cause of

action" under the ICFA, *id.* at 567, even when the defendant systematically breaches many contracts across an entire "prospective plaintiff class," *Greenberger v. GEICO General Insurance Co.*, 631 F.3d 392, 400 (7th Cir. 2011).

ICFA plaintiffs must identify "some stand-alone … fraudulent act or practice," *id.*, and they must also show that the injury they seek to redress was "proximately caused by the alleged consumer fraud." *Connick v. Suzuki Motor Co.*, 675 N.E.2d 584, 594 (Ill. 1996), citing *Stehl v. Brown's Sporting Goods, Inc.*, 603 N.E.2d 48, 51–52 (Ill. App. 1992). ICFA plaintiffs cannot rely on a generalized "market theory" of causation claiming that the defendant "inflate[d] the cost of its product far above what it could have charged had the" defendant not "misled consumers." *De Bouse v. Bayer AG*, 922 N.E.2d 309, 314–15 (Ill. 2009), citing *Oliveira v. Amoco Oil Co.*, 776 N.E.2d 151, 155 (Ill. 2002). To show proximate cause, the "plaintiff must actually be deceived by a statement or omission that is made by the defendant;" the plaintiff cannot rest on vague accusations about inadequate disclosures and resulting price effects in the marketplace. *De Bouse*, 922 N.E.2d at 316.[9]

---

[9] In addition, plaintiffs in Illinois state court must plead fraud under the ICFA with the same level of specificity as under the common law. *Connick*, 675 N.E.2d at 593, citing *People ex rel. Hartigan v. E & E Hauling, Inc.*, 607 N.E.2d 165, 174 (Ill. 1992). As a procedural matter we have held that ICFA complaints alleging an unfair practice in federal court should be judged under Federal Rule of Civil Procedure 8(a) and not the particularity requirement for fraud under Rule 9(b). *Windy City Metal Fabricators & Supply, Inc. v. CIT Tech. Financing Services, Inc.*, 536 F.3d 663, 670 (7th Cir. 2008). The ICFA's heightened state court pleading requirement is still instructive here for two reasons. First, we read the plaintiff banks' complaint as invoking the misrepresentation and fraud line of ICFA cases, and not

As mentioned above, the "any person" language in the ICFA means that businesses can sometimes sue one another under the statute, but a business plaintiff under the ICFA must show a "nexus between the complained of conduct and consumer protection concerns," which we refer to here as the "consumer nexus test." *Athey Products Corp. v. Harris Bank Roselle*, 89 F.3d 430, 437 (7th Cir. 1996). Illinois courts are skeptical of business-v.-business ICFA claims when neither party is actually a consumer in the transaction. ICFA claims may not be available when the business relationship is more like that of "partners" or "joint venturers" and not "consumers of each other's services." See *Cragin Fed. Bank*, 645 N.E.2d at 566, citing *Century Universal Enterprises, Inc. v. Triana Dev. Corp.*, 510 N.E.2d 1260 (Ill. App. 1987). In applying the consumer nexus test, Illinois courts have observed that "there is no inherent consumer interest implicated in a construction contract between a general contractor and a subcontractor," *Peter J. Hartmann Co. v. Capital Bank and Trust Co.*, 694 N.E.2d 1108, 1117 (Ill. App. 1998) (citation omitted), a situation similar to the web of contracts that comprise the card payment system at issue here.

But we need not decide here whether the plaintiff banks could ever establish a consumer nexus in an ICFA data breach claim. As a more preliminary matter, they fail to allege any ICFA violation in this lawsuit that would make that secondary consumer nexus determination necessary.

---

the unfair practice cases, as described below. Second, we read this ICFA requirement as a sign that Illinois courts are cautious in recognizing new kinds of liability under the ICFA. See *Connick*, 675 N.E.2d at 593–94.

3. *Unfair Practice Claim*

The plaintiff banks fail to allege an unfair practice under the ICFA because their theory is essentially a "market theory of causation" argument that Illinois courts have rejected. The complaint alleges that "Schnucks engaged in unfair business practices in violation of [the] ICFA by failing to implement and maintain reasonable payment card data security measures." Am. Compl. ¶ 116. The complaint goes on to allege: "While Schnucks cut corners and minimized costs, its competitors spent the time and money necessary to ensure" the security of "sensitive payment card information." *Id.*, ¶ 118. By not warning consumers or banks of its compromised payment system, this theory goes, Schnucks acted deceptively to maintain its prices and to ensure business as usual until it publicly announced the data breach. See Dkt. 65 at 4.

This argument does not support an ICFA claim. It is very similar to the argument the Illinois Supreme Court rejected in *Oliveira v. Amoco Oil Co.*, where the plaintiff alleged that he paid an "'artificially inflated' price for … gasoline" due to the "defendant's allegedly deceptive advertising scheme." 776 N.E.2d at 155. He also alleged that "all purchasers of Amoco's premium gasolines were injured irrespective of whether [they saw] specific advertisements and marketing materials" because everyone "paid a higher price for the gasoline than they would have paid in the absence of the ads." *Id.* at 156. This could not support an ICFA claim, the Illinois Supreme Court later explained, because "plaintiffs in a class action" under the ICFA "must prove that 'each and every consumer who seeks redress actually saw and was deceived by the statements in question.'" *De Bouse*, 922 N.E.2d at 315, quoting

Barbara's Sales, Inc. v. Intel Corp., 879 N.E.2d 910, 927 (Ill. 2007). General effects on consumer behavior or the price of goods are not enough. See *De Bouse*, 922 N.E.2d at 315.[10]

The plaintiff banks allege that Schnucks effectively manipulated both its prices and sales volume by deliberately concealing the data breach. This manipulation would not have been possible, say the banks, if Schnucks had told the truth about its data security. Dkt. 65 at 4. The banks admit that they did not "plead specific misrepresentations." They argue instead that they do not need to—that alleging an unfair practice directed at the market in general is enough. By simply continuing business as usual as its consultant investigated the data breach, plaintiffs argue, Schnucks violated public policy and by extension the ICFA.[11]

---

[10] In 2006, which was after *Oliveira* but before *De Bouse*, the Illinois Appellate Court found that a consumer could state an ICFA claim where a manufacturer of aluminum-clad wooden windows failed to disclose physical defects in its product. *Pappas v. Pella Corp.*, 844 N.E.2d 995, 1004 (Ill. App. 2006). *Pappas* was not directly addressed by the Illinois Supreme Court in *De Bouse*, where the court relied on its own opinion in *Oliveira* and related cases. See 922 N.E.2d at 314–16. We think the Illinois Supreme Court would take the same approach here and apply *De Bouse* and *Oliveira*, and not *Pappas*, to this case. The plaintiff banks' claim is that Schnucks misrepresented the integrity of its data security policies and thus effectively mispriced its goods in the consumer market. It is not a claim about undisclosed physical product defects. Also, there is no third-party intermediary here, such as a doctor who passed along deceptive information from the defendant. See *De Bouse*, 922 N.E.2d at 318–19.

[11] To characterize their claim as an "unfair practice" rather than a misrepresentation, the plaintiff banks cite a district court decision that in turn quoted *Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 961 (Ill. 2002). *Robinson* adopted a three-factor test employed under the Federal Trade Commission Act in judging unfair practices, but it did not follow

This theory is not consistent with *Oliveira*, which likened its plaintiff's theory to "the fraud on the market theory found in federal securities case law" and rejected it for ICFA claims. 776 N.E.2d at 155 n.1, 164 (internal quotation omitted). An allegation that Schnucks mispriced its products and deceived all of its customers and also the plaintiff banks about its practices must actually identify a deceptive guarantee about data security in order to state an ICFA claim. Plaintiffs have not done so.

4. *Illinois Personal Information Protection Act*

It might be possible for the plaintiff banks to state a different kind of claim under the ICFA by alleging that Schnucks violated the Illinois Personal Information Protection Act by failing to disclose the breach for two weeks after learning of it. A violation of the PIPA can be sufficient to obtain ICFA relief. See 815 Ill. Comp. Stat. 530/20. The data breach occurred in this case, and PIPA requires notice to Illinois residents affected by data breaches. § 530/10. But the plaintiffs failed to explain to the district court whether and how Schnucks' conduct fell under one of the operative subsections of the notice statute and not any of its exceptions.

---

the sort of element-by-element analysis the plaintiff banks seek here. See *id.* at 961–64. Instead, *Robinson* analyzed the unfair practices claims by asking whether a disclosure law or public policy had been violated, see *id.* at 962–63, or whether the plaintiff experienced "oppressiveness and lack of meaningful choice" in a manner similar to a contractual unconscionability claim, see *id.* at 962. The plaintiff banks here do not identify a specific public policy violation or an unconscionability rationale that fits Schnucks' conduct; instead, they maintain that "Schnucks deliberately concealed the ongoing data breach for over two weeks." This is a misrepresentation allegation that claims the consumer market as a whole was deceived. We address it as such.

See *id*. Such an explanation was needed to preserve the PIPA-ICFA claim for appellate review, especially for a counseled class of sophisticated plaintiffs advocating a novel theory.

The problem here is not the adequacy of pleadings but the adequacy of the legal argument in the district court. In responding to a motion to dismiss, "the non-moving party must proffer some legal basis to support his cause of action." *Bonte v. U.S. Bank, N.A.*, 624 F.3d 461, 466 (7th Cir. 2010), quoting *County of McHenry v. Insurance Co. of the West*, 438 F.3d 813, 818 (7th Cir. 2006). Courts "will not invent legal arguments for litigants," even at the motion to dismiss stage, and are "not obliged to accept as true legal conclusions or unsupported conclusions of fact." *County of McHenry*, 438 F.3d at 818 (citations omitted). This need stems not from the modest pleading requirements of Rule 8 but instead from the adversarial process. If a Rule 12 motion to dismiss is filed, plaintiffs must "specifically characterize or identify the legal basis" of their claims or face dismissal; just because the complaint may have complied with Rule 8 does not mean that it is "immune from a motion to dismiss." See *Kirksey v. R.J. Reynolds Tobacco Co.*, 168 F.3d 1039, 1041 (7th Cir. 1999).

This is especially true when a party advances a novel legal theory. See *id.* at 1042 ("a claim that does not fit into an existing legal category requires more argument by the plaintiff to stave off dismissal, not less"). Our situation here is reminiscent of *Kirksey*, where the plaintiff's lawyer seemed to have hoped "that the current legal ferment in the world of tobacco litigation"—or in this case data breach litigation—"will brew him up a theory at some future date if only he can stave off immediate dismissal under Rule 12(b)(6)." *Id.* The failure to respond waives the claim. *Bonte*, 624 F.3d at 466.

The plaintiff banks argue that they asserted this claim properly in the district court. Their support is meager. Plaintiffs point to a footnote in the complaint that refers to a PIPA code section, see Am. Compl. ¶35 n.23, and a page and a half devoted to their ICFA claims in the brief opposing the motion to dismiss, Dkt. 65 at 18–19. These were not sufficient to alert the district court that plaintiffs were even relying on the theory they argue on appeal, let alone to explain the theory to the district court. Though plaintiffs summarized the connections between the federal FTCA and the ICFA, see Am. Compl. ¶ 115, they simply did not address the potential application of PIPA to this case in either filing.

One district court case cited in the plaintiff banks' response mentions PIPA. Even if that were enough to alert the district judge to the issue—and it is certainly not—plaintiffs tried to distinguish that case, not to draw parallels to it. See Dkt. 65 at 18, distinguishing *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518 (N.D. Ill. 2011) (brought by consumers). Rather, they argued that their ICFA "claim should stand for the same reasons as in *Home Depot*," a case that does not mention PIPA or even cite the portion of *Michaels* that discussed PIPA. See *Home Depot*, 2016 WL 2897520, at *6. Nothing in this complaint or the plaintiffs' briefing in the district court fairly alerted the district court that PIPA had any relevance.

We will not revive this potential claim here. "Even if the argument was not waived … the [plaintiffs-appellants] failed to support it in this court with anything more than abstract generalities," which is a sufficient reason not to wade into the issue. *Hassebrock v. Bernhoft*, 815 F.3d 334, 342 (7th Cir. 2016); see also *Voelker v. Porsche Cars North Am., Inc.*, 353 F.3d 516, 527

(7th Cir. 2003) (under Fed. R. App. P. 28, "an appellant's argument must provide both his 'contentions and the reasons for them'" to be considered). Whether—and if so how—a PIPA violation could support an ICFA claim brought by one business against another is a question for another case.

Conclusion

We agree with the district court that neither Illinois nor Missouri would recognize any of the plaintiff banks' theories to supplement their contractual remedies for losses they suffered as a result of the Schnucks data breach. The judgment dismissing the action is

AFFIRMED.