2020

Data Security's Unjust Enrichment Theory

Lior Strahilevitz

Data Security's Unjust Enrichment Theory

Lior Jacob Strahilevitz†

INTRODUCTION

Remijas v Neiman Marcus Group, LLC,[1] is Judge Diane Wood's most famous data security opinion, and for good reason. The opinion is elegantly written and refreshingly pragmatic with respect to an issue that has prompted other courts to fall into the trap of empty formalism. Yet the opinion is not perfect, and this Essay celebrating Wood's silver anniversary on the bench will argue that it missed an opportunity to solve a vexing and important problem that arises when data breach suits are brought in federal court.

I. THE LEGAL BACKDROP FOR *REMIJAS*

Remijas arose out of a significant data breach at the luxury retailer, Neiman Marcus. In December of 2013, Neiman Marcus customers began reporting a spate of fraudulent charges on credit cards used at the store. The retailer initiated an investigation and discovered a few weeks later that malware had been installed on its network, exposing customer credit card numbers and other personally identifiable customer information that was used to make the fraudulent purchases.[2] Some 350,000 credit card customers had their information exposed, and at least 9,200 of those exposed credit cards were used to make fraudulent purchases. In an attempt to placate irate customers, Neiman Marcus "offer[ed] them one year of free credit monitoring and identity-theft protection."[3] Customers who detected fraudulent purchases on their accounts had the charges fully refunded.

The data breach prompted a number of class action suits, including one filed on behalf of Hilary Remijas (a Chicago-based

† Sidley Austin Professor of Law, The University of Chicago Law School. The author thanks the Carl S. Lloyd Faculty Fund for research support and Lee Fennell for helpful comments on an earlier draft.

1 794 F3d 688 (7th Cir 2015).

2 Id at 690.

3 Id.

intellectual property lawyer who shopped at the Neiman Marcus in Oak Brook, Illinois)[4] and three other named plaintiffs. That suit alleged "a number of theories for relief: negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws."[5] But in federal district court, the suit could not even make it past the starting gate—Judge James B. Zagel dismissed Remijas's complaint for lack of Article III standing.[6]

In Judge Zagel's view, each of the four major harms asserted by the plaintiffs failed to satisfy the requirements of Article III. These alleged harms were (1) an increased risk of identity theft in the future stemming from the breach, (2) the time and money spent to reduce the risk of future identity theft, (3) the financial injury from having purchased Neiman Marcus's products on the basis of erroneous assumptions about its data security practices, and (4) a loss of control over and loss of value of the customers' personal information.[7]

Judge Zagel concluded that an increased risk of identity theft failed to establish the requisite level of harm to satisfy Article III because it appeared that more than 97 percent of the customers whose data was stolen were not demonstrably victimized by identity theft.[8] Only those customers who did incur fraudulent charges would be able to demonstrate an Article III injury in fact. Judge Zagel regarded the injury associated with time and money spent to mitigate the risk of future identity theft as de minimis.[9] In his view, "when one sees a fraudulent charge on a credit card, one is reimbursed for the charge, and the threat of future charges is eliminated by the issuance of a new card, perhaps resulting in a brief period where one is without its use."[10] (It appears that Judge Zagel's statement was factually inaccurate as applied to at least a minority of identity theft victims.)[11] Judge Zagel was also

---

4 See DLA Piper, *Hilary Remijas: Attorney*, archived at https://perma.cc/8NCS-ZFXZ; Class Action Complaint, *Remijas v Neiman Marcus Group, LLC*, No 14-CV-01735, *4 (ND Ill filed Mar 12, 2014) (available on Westlaw at 2014 WL 1187603).

5 *Remijas*, 794 F3d at 690–91.

6 *Remijas v Neiman Marcus Group, LLC*, 2014 WL 4627893, *1 (ND Ill).

7 Id at *1–5.

8 Id at *3–4.

9 Id at *4.

10 *Remijas*, 2014 WL 4627893 at *4.

11 See Erika Harrell, *Victims of Identity Theft, 2016* *9 & tbl 7 (Bureau of Justice Statistics, Jan 2019), archived at https://perma.cc/65UX-H5U3 (noting that 12 percent of identity theft victims suffered out-of-pocket losses that were not reimbursed, and that more than 3.5 percent of identity theft victims saw their credit ratings drop, had problems

quick to brush aside the idea that customers' loss of control over their private information was a sufficiently concrete harm to establish standing, suggesting that because the plaintiffs' data had not been sold and the plaintiffs could not have sold this information, there was no concrete injury.[12]

That left one final potential basis for standing: the allegation that the plaintiffs paid a premium at Neiman Marcus and expected that a portion of those funds would go to ensuring adequate data security protections. The complaint articulated the injury this way:

> A portion of the services purchased from Neiman Marcus by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of [personal identifying information], including their credit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from Neiman Marcus.[13]

Judge Zagel wrote that this basis for relief was "creative, but unpersuasive."[14] He was half right. Judge Zagel conceded that the benefit of the bargain / unjust enrichment theory of harm had been applied by the Seventh Circuit in a previous case, *In re Aqua Dots Products Liability Litigation*,[15] but he found the case distinguishable. So let's revisit *Aqua Dots*.

The facts alleged in the *Aqua Dots* complaint are the stuff of parental nightmares. Parents bought kits of brightly colored small beads that would adhere to each other when sprayed with water and that kids could use to form attractive shapes and patterns.[16] The manufacturer of Aqua Dots outsourced production to JSSY Ltd, and JSSY substituted a toxic adhesive for the safer adhesive that the manufacturer had specified.[17] The result was that

---

with their banks, or had to deal with collection agencies because of fraudulent charges made on their existing accounts).

12 *Remijas*, 2014 WL 4627893 at *5. This determination by Judge Zagel is rather puzzling. The fact that a resource is market-inalienable does not mean that if the resource is taken without permission, no injury to a property right has occurred. See generally Margaret Jane Radin, *Market-Inalienability*, 100 Harv L Rev 1849 (1987).

13 Class Action Complaint at *10 (cited in note 4).

14 *Remijas*, 2014 WL 4627893 at *4.

15 654 F3d 748 (7th Cir 2011).

16 See id at 749.

17 Id.

when some kids ingested the colorful beads—as is inevitable with a product like that—they were exposed to a range of consequences from nausea and dizziness to amnesia, loss of consciousness, or death.[18] Once the manufacturer discovered the problem, it recalled the products and gave refunds to customers who asked for them.[19]

Then–Chief Judge Frank Easterbrook, writing for the *Aqua Dots* court, dismissed the manufacturer's argument that the plaintiffs lacked standing—in his view even customers who were not injured suffered an injury in fact. As he saw it, "[t]he plaintiffs' loss is financial: they paid more for the toys than they would have, had they known of the risks the beads posed to children. A financial injury creates standing."[20]

If purchasing crafts products that were less safe than they appeared is a financial injury conferring standing, why aren't the purchases at Neiman Marcus under a false pretense that the company would take reasonable steps to protect customer data a commensurable injury? That is a question that both Judge Zagel in the district court and then–Chief Judge Wood on appeal needed to answer. In the Part below, we'll compare the two judges' explanations for why *Aqua Dots* is inapplicable to the data security context.

II. *AQUA DOTS* AND THE UNJUST ENRICHMENT THEORY

Judge Zagel distinguished *Aqua Dots* from *Remijas* on the basis of a distinction he drew between the intrinsic and extrinsic features of a product. He posited that only failures to deliver on intrinsic characteristics concretely injured a plaintiff. In his view, such a distinction was necessary to establish a limiting principle for *Aqua Dots*.[21] He explained his perspective this way:

> In my view, a vital limiting principle to this theory of injury is that the value-reducing deficiency is always intrinsic to the product at issue. Under Plaintiffs' theory, however, the deficiency complained of is extrinsic to the product being purchased. To illustrate the problem this creates: suppose a retail store does not allocate a sufficient portion of its revenues to providing adequate in-store security. A customer who is

---

18 Id at 749–50.

19 *Aqua Dots*, 654 F3d at 750.

20 Id at 751.

21 *Remijas v Neiman Marcus Group, LLC*, 2014 WL 4627893, *5 (ND Ill).

> assaulted in the parking lot after patronizing the store may well have a negligence claim against the store owner. But could he or she really argue that she overpaid for the products that she purchased? Or even more to the point: even if no physical injury actually befell the customer, under Plaintiffs' theory, the customer still suffered financial injury because he or she paid a premium for adequate store security, and the store security was not in fact adequate.
>
> As set forth in *Aqua Dots*, this theory of injury is plainly sensible. In my view, however, expanding it to include deficiencies extrinsic to the purchased product would effectively render it meaningless.[22]

Unable to differentiate *Remijas* from this parking lot hypothetical, Judge Zagel dismissed the suit.

The following year, when the Seventh Circuit weighed in on *Remijas*, the court reversed Judge Zagel's determination that the plaintiffs lacked standing to sue.[23] It held that he reached the incorrect result both with respect to risk of future harm, and time and money spent mitigating the risk of future identity theft.[24] In Chief Judge Wood's view, both of these harms were adequate injuries to confer standing to sue in federal court. I'll have more to say about this aspect of the opinion momentarily.

Without resolving the question of whether *Aqua Dots* applied to a company's failure to provide adequate data security, Chief Judge Wood expressed the panel's attitude toward the idea—the judges were "dubious."[25] Echoing Judge Zagel, the chief judge noted that the *Aqua Dots* line of cases had involved products liability cases, though nothing in *Aqua Dots* itself indicated that its reasoning was limited to manufacturers. Still, in defense of a limitation, the chief judge added these words:

> Our case would extend that idea from a particular product to the operation of the entire store: plaintiffs allege that they would have shunned Neiman Marcus had they known that it did not take the necessary precautions to secure their personal and financial data. They appear to be alleging some form of unjust enrichment as well: Neiman Marcus sold its products at premium prices, but instead of taking a portion

---

22 Id.

23 *Remijas*, 794 F3d at 697.

24 Id at 696.

25 Id at 694.

> of the proceeds and devoting it to cybersecurity, the company pocketed too much. This is a step that we need not, and do not, take in this case. Plaintiffs do not allege any defect in any product they purchased; they assert instead that patronizing Neiman Marcus inflicted injury on them. That allegation takes nothing away from plaintiffs' more concrete allegations of injury, but it is not necessary to support their standing.[26]

Here we see the panel largely agreeing with the distinction that Judge Zagel identified between intrinsic and extrinsic aspects of a product, with the result being that manufacturers face a kind of liability to which retailers are not exposed.

Neither judge provides a clear explanation for what precisely makes the unjust enrichment theory inapplicable outside the realm of products liability. Judge Zagel's primary concern seems to be the absence of a limiting principle. Chief Judge Wood's concern seems to be that the unjust enrichment allegation is not necessary, and weak in comparison to the other theories of injury. Neither objection holds up especially well under scrutiny. I will identify the problems with Judge Zagel's analysis below, and then take up the issues with Chief Judge Wood's concern in Part III.

The obvious limiting principle for *Aqua Dots* is the materiality of a product or service attribute to the plaintiff's decision to purchase. If the alleged defect would have trivially influenced consumers' purchase decisions, then there is no unjust enrichment, because very few sales at the margins would have depended on the relevant attribute. Whereas the distinction between intrinsic and extrinsic product attributes seems to be empty, materiality has an underlying economic logic to it. Returning to Judge Zagel's example, imagine that a store explicitly promised to devote 5 percent of its revenue to world-class parking lot security, and it in fact spent only 1 percent of its revenue on such security. Customers who paid a 4 percent premium on all products would have been injured economically, regardless of whether they were ever assaulted. To return to the facts of *Aqua Dots*, what is salient about the defendants' conduct there is not that there was a problem with the Aqua Dot physical inputs, but that the substitution of a toxic input for a nontoxic one rendered the Aqua Dots a lethal risk to kids who would play with them. The relevant question is materiality, not whether the attribute is intrinsic to the product.

---

[26] Id at 695 (citation omitted).

The explicit nature of a promise makes it easier to argue that the promise itself was a material part of customer expectations. And indeed, the Neiman Marcus Gift Registry Security and Privacy policy currently on its web site, which was (shockingly) last updated on September 12, 2013, just a few months before the data breach that gave rise to *Remijas* was detected, provides as follows:

> To help us achieve our goal of providing the highest quality products and services, we use information from our interactions with you and other customers, as well as from other parties. Because we respect your privacy, we have implemented procedures to ensure that your personal information is handled in a safe, secure, and responsible manner.[27]

So Neiman Marcus was making an explicit promise that it would keep its customers' credit card information secure, a standard its data security practices quite plausibly breached. The only open questions are whether such promises were relied upon by reasonable consumers, or whether Neiman Marcus's apparently inadequate data security practices were a matter about which most consumers would have been indifferent.

An analogy to counterfeit goods is helpful here. Suppose someone purchased a large number of printer cartridges that were supposedly made by the well-regarded company that manufactured her printer. And suppose it later turned out these cartridges were counterfeit. The consumer would be able to recover on an unjust enrichment theory simply because the goods were counterfeit and misrepresented to be authentic.[28] There would be no need for the plaintiff to demonstrate that the counterfeit goods were inferior in quality to the genuine article or that they would be worth less on the resale market. The customer wanted name-brand items and the defendant instead delivered cheaper alternatives that were hard to distinguish from the real deal. How is what Neiman Marcus did analytically distinct?

The available data suggests that data security is a relevant factor for a sizeable minority of consumers when deciding to obtain a credit card. A recent survey of one thousand American adults revealed that the single most widely identified reason for obtaining a credit card was to build up a positive credit score, an

---

[27] Neiman Marcus, *Neiman Marcus Gift Registry: Security & Privacy Information* (Sept 12, 2013), archived at https://perma.cc/3SLP-HPAJ.

[28] See, for example, *Papergraphics International, Inc v Correa*, 910 A2d 625, 627 (NJ Super App Div 2006).

objective that can be compromised by credit card fraud that goes undetected; fully 64 percent of consumers flagged this rationale.[29] Fraud protection was identified as the ninth most salient factor in consumers' use of credit cards, among over a dozen possibilities, helping to explain 23 percent of consumers' actions.[30] Similarly, among the perceived drawbacks of having a credit card, the fear of identity theft ranked ninth out of the twelve most commonly stated concerns, with 29 percent of consumers expressing this anxiety.[31]

There's another point that drives the inadequacy of the *Remijas* district court's analysis home. Hilary Remijas used her *Neiman Marcus* credit card to purchase items at the defendant's stores.[32] Presumably a lot of other plaintiffs in the class did as well. Even if we apply Judge Zagel's intrinsic versus extrinsic distinction, proper data security protocols would be an intrinsic attribute of the store's branded credit card, not an extrinsic one. A credit card that regularly presents consumers with the annoyance of improper charges is not one that many consumers would readily sign up for—the whole point of a credit card is to be billed for goods and services that were actually purchased by the card holder and not to be billed for goods and services that were not lawfully purchased.

In 2020, the Ninth Circuit parted ways with the Seventh Circuit's *Remijas* dicta, albeit without citing the earlier case. *In re Facebook, Inc Internet Tracking Litigation*[33] involved Facebook's surreptitious use of plug-ins to track user browsing activities on third-party web sites. Facebook then packaged and sold information about consumer internet browsing practices.[34] There was no allegation that the consumers in that case suffered pecuniary harms as a result of this tracking, but the plaintiffs did allege that Facebook profited by violating internet users' privacy in a manner that increased Facebook's revenues and contradicted the promises made in Facebook's privacy policies.[35] The Ninth Circuit held that the plaintiffs' unjust enrichment allegations were adequate to establish federal standing because unjust enrichment is

---

29 The Ascent, *Why Swipe? American Credit Card Preferences and Habits by Generation* (Mar 5, 2019), archived at https://perma.cc/RSH2-PLLL.

30 Id.

31 Id.

32 See *Remijas*, 794 F3d at 691.

33 956 F3d 589 (9th Cir 2020).

34 See id at 596–97.

35 Id at 598–602.

recognized as a harm under California law.[36] Though Illinois law is less well developed than California law with respect to unjust enrichment claims of this kind, the same result would plausibly hold under Illinois law as well.[37] The unjust enrichment analysis would be identical in the privacy and data security contexts—in both instances, plaintiffs are being exposed to unnecessary and undesired risks involving unauthorized access or use of sensitive information. *In re Facebook* thus shows the viability of the path not taken by the Seventh Circuit in *Remijas*.

III. WRONG REASONS AND RIGHT RESULTS

Chief Judge Wood's opinion in *Remijas* is more famous for the theories of standing that it recognized than for the one it rejected. Indeed, the panel rejected Judge Zagel's determination that an enhanced risk of identity theft and the mitigation strategies reasonably prudent consumers would pursue to prevent future identity theft stemming from a data breach did not constitute injuries in fact. She took Judge Zagel to task for his determination that there was no substantial risk to consumers if their losses from identity theft would be reimbursed by their credit card issuers.[38] In her view, the reason why hackers would break into Neiman Marcus's database was clear—"the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[39] She correctly noted that some of Neiman Marcus's customers could be victimized by identity theft in the year after the breach—the 9,200 cards exposed in the breach that were subject to fraudulent charges were just the identified accounts as of the time the complaint was filed.[40]

The major fly in the ointment for her take on *Remijas* is the absence of a control group. In 2018 alone, nearly 450,000

---

36 Id at 599–601.

37 Under Illinois law, unjust enrichment can arise where the plaintiff alleges that the defendant retained a benefit to the plaintiff's detriment in a way that violates "principles of justice, equity, [or] good conscience." *Apollo Real Estate Investment Fund, IV, LP v Gelber*, 935 NE2d 949, 962 (Ill App 2009). The defendant must owe the plaintiff an independent duty in order for there to be a recovery. *Martis v Grinnell Mutual Reinsurance Co*, 905 NE2d 920, 928 (Ill App 2009). It seems uncontroversial that Neiman Marcus owed its customers a duty, so the most relevant questions would be whether the harms suffered by Neiman Marcus's customers count as a "detriment" to them and whether those harms arose because of the defendant's breach of a contract implied in law.

38 *Remijas*, 794 F3d at 693 ("[T]he Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing.").

39 Id.

40 Id at 693–94.

instances of identity theft were reported to the Federal Trade Commission, including more than 150,000 cases of credit card fraud.[41] This statistic almost certainly reflects an undercount, however, as surveys indicate that 35 percent of Americans have been victims of credit card fraud at some point in their lives, including roughly one-third of millennials, who have not had credit cards for substantial periods of time.[42] A different 2016 survey revealed that 5.3 percent of American adults (and 7.5 percent of those with credit cards) had been victims of credit card fraud in the past twelve months.[43] If the baseline rate of credit card fraud is 4 percent, and in the months following the Neiman Marcus breach about 2.5 percent of the consumers whose information was compromised were victimized by identity theft, then it is hard to make a convincing argument that the plaintiffs faced an elevated risk because of the breach. It's a fair question whether skepticism about causation belongs in the standing analysis—which determines whether the plaintiffs can sue—as opposed to the liability analysis. Other federal courts have struggled with this difficult issue.[44] The mix of false positives and false negatives with respect to data breaches makes this context a particularly attractive vehicle for imposing damages based on the elevated risk of future harm rather than trying to provide full compensation to people who are victimized by identity theft and no compensation to people who aren't.[45]

Chief Judge Wood was on firmer footing when she reversed Judge Zagel's determination that the costs of mitigating the consequences of the breach were not concrete injuries that conferred standing. Indeed, one factor mitigating the Neiman Marcus credit card theft's impact was that presumably a lot of customers cancelled their compromised credit cards before they were used successfully by criminals. Time is money, as the old saying goes, and the opportunity cost of having to prevent identity theft after

---

41 See Federal Trade Commission, *Consumer Sentinel Network: Data Book 2018* *8 (Feb 2019), archived at https://perma.cc/5BKW-2SK8.

42 Lyle Daly, *Identity Theft and Credit Card Fraud Statistics for 2019* (The Ascent, Nov 7, 2019), online at https://fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics (visited Mar 15, 2020) (Perma archive unavailable).

43 Harrell, *Victims of Identity Theft* at *4 tbl 2 (cited in note 11).

44 See, for example, *Beck v McDonald*, 848 F3d 262, 270–76 (4th Cir 2017); *Resnick v AvMed, Inc*, 693 F3d 1317, 1323–24 (11th Cir 2012); *Reilly v Ceridian Corp*, 664 F3d 38, 42–43 (3d Cir 2011); *Krottner v Starbucks Corp*, 628 F3d 1139, 1141–43 (9th Cir 2010).

45 For a well-developed proposal along these lines, see Ariel Porat and Alex Stein, *Liability for Future Harm*, in Richard Goldberg, ed, *Perspectives on Causation* 221, 228–36 (Hart 2011).

receiving a breach notification is economically significant.[46] According to a Bureau of Justice Statistics report, approximately 43 percent of identity theft victims who had a single account targeted had to spend more than a day making calls and writing letters to clear up the problems created by this fraud.[47] Victims who experienced only credit card fraud spent on average three hours fixing the resulting problems.[48] This is not a de minimis harm—it's the kind of harm that class actions were designed to deter. Taking judicial notice of publicly available statistics like these—the Bureau of Justice Statistics has been posting similar statistics for years[49]—would have been adequate to illustrate that the mitigation costs associated with data breaches are concrete injuries. Even though it is not clear that victims of the Neiman Marcus hack faced a demonstrably elevated risk of credit card fraud, a null effect of the breach is not something that a reasonable consumer would have been able to predict ex ante, and there may have been a connection between the precautions that some customers took and the relatively low prevalence of identity theft in *Remijas*. Accordingly, it was still prudent for consumers to start monitoring their credit and taking steps to protect it as soon as they received notice from Neiman Marcus that their data potentially had been compromised.

Chief Judge Wood chose a more fraught path to reach the right conclusion. She counted Neiman Marcus's offer of one year of credit monitoring and identity theft protection to its customers against the company.[50] She explained that this is a service for which interested consumers have to pay nearly twenty dollars a month under ordinary circumstances. So, the fact that Neiman Marcus thought it wise to purchase the service for consumers

---

46 For an in-depth discussion of how to evaluate the economic costs of wasted time, see Adam M. Samaha, *Death and Paperwork Reduction*, 65 Duke L J 279, 319–44 (2015).

47 See Harrell, *Victims of Identity Theft* at *11 & fig 5 (cited in note 11).

48 Id at *12.

49 See generally, for example, Lynn Langton and Michael Planty, *Victims of Identity Theft, 2008* (Bureau of Justice Statistics, Dec 2010), archived at https://perma.cc/27FW-F356.

50 *Remijas*, 794 F3d at 694:

> An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.

illustrated the presence of a concrete injury. It's tempting to call out the apparent inconsistency in Neiman Marcus's position, but this part of the ruling creates perverse incentives for firms, whose prudent mitigation efforts might now enhance their legal liability rather than diminish it. In any event, the empirical evidence suggests that offering credit monitoring services to victims of a data breach reduces by a factor of six the chances that firms that have suffered a breach will be sued.[51] So when a firm like Neiman Marcus makes that offer after a breach they may well be acting pragmatically rather than conceding that the victims have suffered a substantial injury.

To summarize my assessment of *Remijas*, then, it seems that the Seventh Circuit got the outcome right on the question of whether data breach mitigation gives rise to a concrete injury, but adopted the wrong rationale. And the court erred with respect to whether the risk of identity theft associated with the Neiman Marcus breach was significant enough to show that members of the class faced an elevated risk of credit card fraud compared to people whose data was not breached, recognizing standing where the facts to support it were problematic. On the other hand, the court improperly expressed skepticism about the unjust enrichment theory, narrowing an existing Seventh Circuit precedent without a justification grounded in the economics or psychology of consumer purchasing decisions. A stronger opinion in *Remijas* would have affirmed with respect to the harm of elevated identity theft risk and reversed with respect to unjust enrichment.

The preceding analysis raises an inevitable "so what" question. Chief Judge Wood reversed Judge Zagel, and I'd have done the same, albeit on different grounds. It turns out that the reasoning employed on standing does matter significantly, so the question of which theories of harm and injury get embraced or rejected is hardly academic. To fully understand why the standing analysis matters, it will be necessary to peek ahead chronologically and see what happened to *Remijas* on remand.

IV. *REMIJAS*'S AFTERMATH

Judge Zagel was done with *Remijas* after Chief Judge Wood and her colleagues had their say. The case was sent to Judge Samuel Der-Yeghiayan on remand, but he retired before ruling on the

---

[51] See Sasha Romanosky, David Hoffman, and Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J Empirical Legal Stud 74, 90 (2014).

parties' joint motion to approve a class action settlement.[52] The pending motions were transferred to Judge Sharon Johnson Coleman, and she threw out the settlement by decertifying the class. She did so on the grounds that there was a fundamental conflict among the members of the class, who would receive different compensation based on whether (a) they made their purchases at a time when the malware was active on Neiman Marcus's systems and (b) whether their data was compromised by the hackers.[53] Under the terms of the settlement, only those customers whose data was compromised would receive monetary compensation. The settlement class, after all, included some plaintiffs who had purchased products from Neiman Marcus during the period when the malware was active and others who had purchased products after the malware had become inactive.[54] This settlement structure seemed dictated by the bases for standing that the Seventh Circuit had recognized—people whose data was not compromised by the breach would not have an elevated risk of identity theft, nor would it be prudent for them to make expenditures to guard against any increased chance of a breach.

Embracing the unjust enrichment theory of data breaches would have ameliorated these class conflicts, presumably preventing class decertification. Under the unjust enrichment theory, all members of the class would have suffered a concrete injury—Neiman Marcus failed to deliver on its promise to protect customer data, a promise that plausibly helped induce customers to spend their money at Neiman Marcus's stores (and in some cases induced them to obtain a Neiman Marcus credit card as well). Indeed, under this account, any customer who shopped at the store during a period of inadequate security would be entitled to recovery, including those who made purchases at a time when the malware could have compromised the company's databases but didn't. By cutting off the recovery prospects for consumers who got a raw deal as a result of Neiman Marcus's apparently inadequate investments in data security, the Seventh Circuit's decision had the effect of shrinking the size of the class action and substantially reducing the potential liability for firms. In short, Chief Judge Wood's hostility to the plaintiffs' most expansive theory of liability created substantial problems down the road. And

---

52 *Remijas v Neiman Marcus Group, LLC*, 341 F Supp 3d 823, 825 (ND Ill 2018).

53 Id at 826–29.

54 Id at 826–28.

these problems were not just evident in hindsight. They were foreseeable at the time too.

Data breaches entail real harms—annoyances, stress, inconvenience, and uncertainty. They chill commerce, and they can create negative externalities when consumers are unable to trace an instance of identity theft to a particular breach and defendant.[55] The harms from a breach are not limited to identity theft for an unlucky few whose information is compromised.[56] Given that reality, it's a mistake for the legal system to get hung up on injury traceability—as *Remijas* and other cases have done.[57] Such a focus wastes resources and ignores spillover effects, compromising the overarching goal of adequate deterrence. The three consequences for firms that suffer data breaches are (a) class action litigation, (b) potential investigations by the Federal Trade Commission and state attorneys general, and (c) a drop in stock prices.[58] Much of the third punishment is parasitic on the first two, though a data breach may also provide a signal that a firm is mismanaged in other respects. The straightforward application of *Aqua Dots*'s rule to the information economy would have allowed for much more muscular deterrence of lax corporate security. The Seventh Circuit's reluctance to follow *Aqua Dots* to its logical conclusion with respect to a material aspect of consumer purchasing decisions is hopefully a decision that will be revised in time.

---

55 See generally Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur, *Taking Data out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information* (Association for Computing Machinery, April 2020), archived at https://perma.cc/RS78-KUD2.

56 See Daniel J. Solove and Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex L Rev 737, 782–85 (2018).

57 Section 5 of the Federal Trade Commission Act intelligently incorporates this insight. In cases involving consumer deception in trade by a firm, the agency needs to demonstrate a material representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances. See Federal Trade Commission, *FTC Policy Statement on Deception* *2 (Oct 14, 1983), archived at https://perma.cc/V4KN-WJCS. The agency needs to show a substantial injury to consumers in order to prevail on an unfairness claim under § 5 but need not show one to prevail on a deception claim. See 15 USC § 45(n).

58 For a discussion of stock market declines stemming from data breach notifications, see generally Ashish Garg, Jeffrey Curtis, and Hilary Halper, *Quantifying the Financial Impact of IT Security Breaches*, 11 Info Mgmt & Computer Security 74 (2003).

CONCLUSION

In *Remijas v Neiman Marcus Group, LLC*, the Seventh Circuit sensibly and appropriately recognized that the kinds of injuries that follow a data breach can establish standing to sue in federal court. Writing for the court, Chief Judge Wood was pragmatic and wise in deciding that the inconvenience of having to deal with the fallout of a breach was a palpable harm even if the credit card issuer ultimately did not hold a consumer responsible for fraudulent charges made to an account. Yet the court blinked when asked to apply its own precedent in a manner that would punish companies that charge a premium price and deliver a bargain-basement service that falls below industry standards where data security is concerned.[59] Consequential dicta effectively shrunk the class of consumers who would be entitled to monetary compensation following a breach. Predictably, this spelled trouble for a broad-based class action suit and eventually resulted in the decertification of an existing class on remand.

It is often difficult to trace a particular breach to an instance of data misuse. Data breaches are becoming quite common, and the same personal information is often duplicated in a wide variety of databases. The legal system ought to shift its attention from causation toward material misrepresentation—and conclude that charging consumers for adequate data security and failing to deliver on that promise is a harm. It is encouraging to see that the federal courts are finally recognizing this principle—as the Ninth Circuit did in *In re Facebook, Inc Internet Tracking Litigation*—but it's a pity the Seventh Circuit missed the opportunity to get there five years sooner by following *Aqua Dots* to its logical conclusion. Consumers are entitled to a refund regardless of whether they themselves suffered an identity theft that can be traced to a particular breach. Every data breach creates negative externalities, affecting the willingness of consumers to participate fully in the country's economic life and making it that much harder to isolate cause and effect when breaches do occur. If the Seventh Circuit has a second chance to consider the unjust enrichment theory of data breaches, it should set aside *Remijas*'s hasty dicta and embrace the claim as a basis for generating appropriate incentives for firms to protect consumers' personal information.

---

[59] For a helpful discussion of the role of industry standards for data security, see William McGeveran, *The Duty of Data Security*, 103 Minn L Rev 1135, 1195–1207 (2019).