SMU | Dedman School of Law

SMU Law Review

Volume 71 | Issue 2 Article 11

2018

Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases

Jennifer Wilt
Southern Methodist University, jwilt@mail.smu.edu

Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases

*Jennifer Wilt**

In *In re SuperValu, Inc.* (subsequently referred to as *Alleruzzo*), the Eighth Circuit deepened the circuit split on the issue of whether the substantial risk of future identity theft is sufficient to establish the injury-in-fact prong of standing.[1] In *Clapper v. Amnesty Int'l USA*, the Supreme Court addressed substantial risk of injury as a basis for standing.[2] The Court held that the future injury alleged in the complaint was insufficient for standing because it "relie[d] on a highly attenuated chain of possibilities."[3] Several circuits, coming to varying conclusions, have applied *Clapper* in data breach cases to determine whether the increased risk of future identity theft is sufficient to satisfy the injury-in-fact requirement.[4] In *Alleruzzo,* the court applied *Clapper* to hold that fifteen of the named plaintiffs had not alleged a substantial risk of future identity theft sufficient for standing.[5] The Eighth Circuit was correct in its holding because limiting the application of substantial risk as a basis for standing simplifies the analysis and prevents generalized claims from making it into the courts. Particularly in the context of data breaches, limitations must be placed on the standing doctrine to prevent wasting judicial resources.

In the summer of 2014, retail grocery stores operated by SuperValu suffered two cyberattacks on their computer network that processed customers' payments.[6] As a result of the breaches, hackers gained access to customers' names, credit or debit card numbers, card expiration dates, card verification value codes, and personal identification numbers.[7] The plaintiffs were customers who shopped at SuperValu stores using a credit

* J.D. Candidate, SMU Dedman School of Law, May 2019; M. Ed. University of North Texas, May 2015; B.A. University of Oklahoma, December 2011. The author would like to thank everyone who supported her decision to attend law school.

1. *See* 870 F.3d 763, 769 (8th Cir. 2017).
2. *See* 568 U.S. 398, 401 (2013).
3. *Id.* at 410.
4. *Alleruzzo*, 870 F.3d at 769.
5. *Id.* at 771.
6. *Id.* at 765–66.
7. *Id.* at 766.

or debit card.[8] Fifteen of the sixteen named plaintiffs alleged substantial risk of future identity theft, claiming that they had spent time determining if their cards were compromised and monitoring account information.[9] Only one plaintiff alleged a fraudulent charge following the breach.[10]

The customers affected by the data breaches alleged that SuperValu had failed to adequately protect customers' card information and failed to conform to best practices and industry standards for merchants accepting payment by credit or debit card.[11] As a result, the plaintiffs were exposed to the "imminent and real possibility of identity theft."[12] The district court granted SuperValu's motion to dismiss based on the plaintiffs' failure to allege an injury in fact sufficient for standing.[13] In determining standing, the district court considered the sixteen named plaintiffs' claims collectively and concluded that a single fraudulent charge alleged by only one plaintiff was insufficient.[14] The plaintiffs appealed this decision based on their theory of substantial risk of future identity theft.[15]

On appeal, the Eighth Circuit affirmed the dismissal of the fifteen named plaintiffs who alleged only the substantial risk of future identity theft and reversed the dismissal of the named plaintiff who alleged a fraudulent charge on his account.[16] The Eighth Circuit affirmed the dismissal of the claims alleging substantial risk of future injury for two primary reasons. First, the allegations that plaintiffs' information had been misused were too speculative.[17] In supporting their theory of injury, the plaintiffs alleged that illegal websites were selling their information and that their financial institutions were attempting to mitigate the risk, which the court rejected as a basis for standing.[18] Second, the court determined that the theft of plaintiffs' credit or debit card information did not create a substantial risk of future injury, and the costs of mitigating any supposed risk were insufficient to create an injury in fact.[19]

In analyzing the issue of substantial risk, the court emphasized the absence of risk where the stolen information merely consists of credit card information.[20] Since this information alone cannot be used to open new accounts, there is little risk that anyone will use the stolen information to commit any fraud.[21] Despite the relatively low bar for standing at the

8. *Id.* at 767.
9. *Id.*
10. *Id.*
11. *Id.* at 766.
12. *Id.*
13. *Id.* at 767.
14. *Id.* at 768.
15. *Id.* at 768–69.
16. *Id.* at 774.
17. *Id.* at 770.
18. *Id.*
19. *Id.* at 770–71.
20. *Id.*
21. *Id.* at 770.

pleading stage, the court reasoned that "[i]t is possible that some years later there may be more detailed factual support for plaintiffs' allegations," but that support is absent here and "mere possibility" is insufficient.[22] The court also rejected the plaintiffs' allegations of mitigating the risk of identity theft as sufficient to create injury in fact because the plaintiffs failed to allege a substantial risk in the first place.[23] Therefore, the plaintiffs cannot manufacture standing by spending time and money protecting against a speculative threat.[24]

In addressing the circuit split, the court noted that other circuits have applied *Clapper* to find standing where an increased risk of future identity theft is alleged.[25] The court declined to address the varying outcomes based on its conclusion that "the cases ultimately turned on the substance of the allegations."[26] The court referred to *Remijas v. Neiman Marcus Group*[27] in its analysis for the proposition that a complaint can plausibly allege that the theft of financial information creates substantial risk, but it distinguished—without much explanation—the plaintiffs' claims.[28] In *Remijas,* the court held that the plaintiffs' allegations of lost time and money as a result of their credit card information being stolen in a data breach were sufficient to demonstrate a substantial risk of harm.[29] The court reasoned that the risk was substantial since customers' information had already been stolen and 9,200 customers had already incurred fraudulent charges.[30] The *Remijas* court noted that requiring plaintiffs to wait until hackers actually commit fraud could create more standing problems down the road because it becomes harder to trace the injury to the initial breach.[31] Though the Eighth Circuit did not discuss the *Remijas* case beyond a passing mention, the reasoning in *Alleruzzo* suggests a fundamental disagreement in assessing the risk of stolen credit card information since the court outright rejected the notion that breach alone was sufficient for standing.[32]

The court also cited *Beck v. McDonald*[33] to support the idea that stolen credit card information does not pose a threat significant enough to constitute a substantial risk.[34] In *Beck*, the Fourth Circuit rejected a substantial risk of future injury claim as too speculative.[35] Veterans receiving medical treatment filed suit when a laptop with unencrypted patient in-

22. *Id.* at 771.
23. *Id.* at 771–72.
24. *Id.*
25. *Id.* at 769.
26. *Id.*
27. *See generally* 794 F.3d 688 (7th Cir. 2015).
28. *Alleruzzo*, 870 F.3d at 770.
29. *Remijas*, 794 F.3d at 692, 696.
30. *Id.* at 692.
31. *Id.* at 693.
32. *Alleruzzo*, 870 F.3d at 770–71.
33. *See generally* 848 F.3d 262 (4th Cir. 2017).
34. *Alleruzzo*, 870 F.3d at 771.
35. *See Beck*, 848 F.3d at 274.

formation was stolen from the facility.[36] The stolen information included the patients' names, birth dates, last four digits of social security numbers, and physical descriptors.[37] In finding that the "mere theft of these items, without more, [could not] confer Article III standing,"[38] the court relied on the fact that no evidence of misuse or identity theft had been discovered at that point in the case, despite extensive discovery.[39] The *Alleruzzo* court seems to have used similar reasoning—since there was little to no risk that identity theft would occur, the risk was minimal and so standing on the basis of substantial risk could not be found.[40]

The Eighth Circuit came to the correct conclusion in finding that the plaintiffs named in *Alleruzzo* failed to allege a substantial risk of future injury sufficient to establish an injury in fact.[41] The allegations are too speculative—the risk that one *might* experience credit card fraud is insufficient. An even more problematic aspect of the substantial risk of future harm allegations is that the potential for credit card fraud hardly seems substantial in a day and age where credit card numbers are stolen all the time and companies actively monitor for this activity.[42] The risk seems especially minimal in light of the fact that cancelling credit cards is a relatively easy process and banks often reimburse customers for fraudulent charges.[43] Thus, the only expense is mere inconvenience or fear.[44] Allowing these claims to provide standing runs the risk of allowing generalized claims into court. In *Lujan v. Defenders of Wildlife*, the Supreme Court rejected similar types of claims that would have allowed virtually anyone with an interest in the subject matter of the suit who alleged that their interest would be negatively impacted to establish injury in fact.[45] The *Alleruzzo* plaintiffs' theory of injury is similar to the claim rejected in *Lujan*—they want anyone connected to the data breach to have standing, regardless of whether injury is likely or imminent—but it is entirely too speculative to suggest that anyone who charges their credit card in a store that experiences a breach has suffered an injury in fact.[46] Though immi-

36. *Id.* at 267.
37. *Id.*
38. *Id.* at 275.
39. *Id.* at 274.
40. *In re* SuperValu, Inc. (*Alleruzzo*), 870 F.3d 763, 770–71 (8th Cir. 2017).
41. *Id.*
42. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) (explaining that "[h]ackers are constantly seeking to gain access to the data banks of companies . . ." and that hacked companies often provide free services to monitor hacked customers' accounts).
43. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 30 (2007) (explaining that existing laws limit consumer liability in the event of fraud and that many companies "voluntarily cover all fraudulent charges").
44. *But see* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (reasoning that generalized anxiety and stress resulting from data breach is sufficient to create an injury in fact).
45. *See* 504 U.S. 555, 563, 566 (1992) (involving a challenge to a statute that interfered with plaintiffs' ability to observe the habitats of various endangered species).
46. *In re* SuperValu, Inc. (*Alleruzzo*), 870 F.3d 763, 769–70 (8th Cir. 2017).

nence is an "elastic concept," it would be stretched too far if individuals who have suffered inconvenience, at most, were allowed to move forward.[47]

At the pleading stage, the threshold for establishing standing should be low so that individuals are permitted to bring claims when they have suffered harms.[48] Striking the appropriate balance between allowing those who have been exposed in a data breach to bring claims and dismissing generalized claims is particularly precarious when the plaintiffs have alleged substantial risk of future injury. On the one hand, requiring more specific details of how the plaintiffs will suffer harm in the future helps to keep trivial claims out of the courts. On the other hand, requiring more factual allegations at the pleading stage to allege a minimum injury only creates—as the *Lujan* dissent describes it—an "empty formality."[49] The Eighth Circuit skirted around the issue by stating that it may be "possible that some years later there may be more detailed factual support for plaintiffs' allegations of future injury," but the current support is lacking.[50] The court should not have kept the door open to future injury claims in breaches involving only credit card information. The entire analysis rejects the plaintiffs' theory of standing because there is minimal risk, but then the court chose to avoid creating precedent that rejects standing in future injury cases entirely.[51] But the court's analysis was sound—only cases that have alleged substantial risk should go forward, and cases involving the theft of credit card information simply do not involve substantial risk. Further, the suggestion is misleading because it becomes more likely that plaintiffs will have difficulty establishing the traceability element of standing as more time passes.[52]

The court implied that substantial risk of future injury would be sufficient for standing in cases involving personal information.[53] Though the court does not rely on this premise to reject the plaintiffs' claims, the distinction between personal information and credit card information is an important one.[54] As the court noted, when credit card information is stolen, there is little risk of identity theft because unauthorized accounts cannot be opened with credit card numbers alone.[55] And so, when credit card information alone is stolen, the only risk is fraudulent charges, which

47. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

48. *See Lujan*, 504 U.S. at 561 (explaining that plaintiffs may allege general factual allegations at the pleading stage but must provide "specific facts" at the summary judgment stage).

49. *Id.* at 592 (Blackmun, J., dissenting).

50. *Alleruzzo*, 870 F.3d at 771.

51. *See id.* at 770–72.

52. *See Lujan*, 504 U.S. at 560–61 (explaining the elements of standing); *see also Clapper*, 568 U.S. at 413 (reasoning that plaintiffs would not be able to establish causal connection because they could only speculate as to whether the injury would occur).

53. *See Alleruzzo*, 870 F.3d at 770–71.

54. *See id.*

55. *See id.* at 770.

can often be easily remedied without court intervention.[56] However, where personal information is involved—social security numbers, birth dates, or driver's license numbers—the risk of identity theft is substantial since criminals can use the information to open unauthorized accounts.[57] Further, the risks would be more difficult to prevent and remedy.[58] Not to mention, the risk remains potentially forever.[59]

In comparing the types of data stolen, the court's reliance on *Beck* seems misguided. Despite the fact that the stolen information was personal, the *Beck* court determined that there was not a substantial risk of future injury because there was no evidence of misuse following extensive discovery.[60] But this seems too harsh for an injury-in-fact analysis, especially at the pleading stage.[61] For starters, the passage of time would not provide much comfort to individuals who have had such sensitive information stolen. Additionally, the *Beck* court's concern with the passage of time seems more appropriate in determining the causal connection component of standing.[62] As time passes, the connection between the breach and the fraudulently used information may be more difficult to establish, but this analysis is inappropriate in assessing the injury-in-fact element.

Other circuits have relied on the distinction between stolen credit card information and stolen personal information in assessing substantial risk of future injury. The Second Circuit rejected claims of substantial risk of future injury where the data breach only involved credit card information.[63] Notably, the plaintiff had experienced a fraudulent charge, but her bank repaid it and the plaintiff had cancelled her card so there was no risk of future fraud.[64] This approach is sound—a plaintiff should not be allowed to proceed where the court will not need to address any sort of present injury. The Sixth Circuit held that allegations of substantial risk of future harm were sufficient for standing where the information stolen from an insurance company included existing and potential customers' birth dates, social security numbers, and driver's license numbers.[65] The

56. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, supra note 43, at 30 (explaining that existing laws limit consumer liability for fraudulent charges and that credit and debit card companies often voluntarily cover fraudulent charges).

57. *See Alleruzzo*, 870 F.3d at 770; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 43, at 9 (explaining how personally identifying information can be used to open new accounts or incur charges on existing accounts and, further, that identity theft victims may be unaware of identity theft for longer periods of time, thus causing them to "face substantial costs and inconvenience repairing damage to their credit records").

58. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 43, at 28–29 (explaining the difficulty in determining the link between breach and identity theft because it is difficult to determine how the data was obtained and identity thieves may wait to commit fraud).

59. *See id.* at 29.

60. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

61. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992); *Alleruzzo*, 870 F.3d at 768.

62. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 412–13 (2013) (reasoning that plaintiffs could not establish causal connection where they could only speculate that injury would occur).

63. Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

64. *Id.*

65. Galaria v. Nationwide Mut. Ins., 663 F. App'x 384, 386, 388 (6th Cir. 2016).

court inferred substantial risk from the mere fact that personal information was stolen, reasoning that it would be unreasonable to require plaintiffs to wait for actual misuse.[66]

In the narrow context of determining if a substantial risk of future injury exists in data breach cases, courts should distinguish the types of information stolen. Where the breach has resulted in stolen credit card information, the claims should be dismissed because there is no substantial risk and, therefore, no injury in fact. But where the breach has resulted in stolen personal information, the claims should be presumed to establish substantial risk sufficient for injury in fact. In other words, the mere fact of the breach establishes injury in fact where personally identifying information is involved.[67] Arguably, such a presumption would create generalized standing, but this risk seems minimal considering such claims would be rejected where the other elements of standing could not be established.

The holding in *Alleruzzo* deepens the circuit split regarding whether substantial risk of future injury is sufficient to confer standing in data breach cases. While some courts have been too lenient in allowing claims to go forward, others have been too strict in dismissing meritorious claims. A more straightforward approach is necessary to help courts grapple with the increasing number of data breach cases. In light of the recent breach of Equifax, courts will need more streamlined methods to assess standing.[68] Presumably, many suits will be filed in the coming months and so the urgency of clarifying the injury-in-fact analysis in data breach cases is even more pressing.[69]

66. *Id.* at 388.

67. *See* Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (holding that substantial harm exists where personally identifying information is stolen "by virtue of the hack").

68. *See Credit Reporting Agency Equifax Suffers Hack Affecting 146 Million*, TICKER (Sept. 25, 2017), http://theticker.org/credit-reporting-agency-equifax-suffers-hack-affecting-146-million [https://perma.cc/S3BZ-FRAN] (describing the breach affecting the personal information of over 143 million Americans at Equifax, one of three major consumer credit reporting agencies).

69. *See* Scott Cole & Associates, *Scott Cole & Associates Files Class Action Lawsuit Against Equifax for Data Breach*, PR NEWSWIRE (Sept. 28, 2017), https://www.prnewswire.com/news-releases/scott-cole—associates-files-class-action-lawsuit-against-equifax-for-data-breach-300520112.html [https://perma.cc/G939-P7VT].