Articles + Publications | January 24, 2022

The Supreme Court's *Ramirez* Isn't Standing in the Way of Standing in Recent Data Breach and Privacy Cases

Privacy & Cybersecurity Newsletter

WRITTEN BY

Lindsey E. Kress | Molly McGinnis Stine | Tara L. Trifon

Despite the much-anticipated impact of *TransUnion LLC v. Ramirez*[1] ("*Ramirez*"), the Supreme Court decision has not prevented data breach and privacy class actions from proceeding past the pleading stage in federal courts across the country. Instead, recent rulings indicate that courts are willing to find general allegations of actual or future harm (such as increased risk of identity theft and invasion of privacy) sufficient to state a claim at the pleading stage – at least where the plaintiffs allege that their personal information was actually accessed and/or misused.[2]

There seem to be several reasons for this trend. First, as most district courts have pointed out, *Ramirez* was decided after a trial, thereby providing the court with an established factual record. Most of the recent cases, on the other hand, are being considered at the motion to dismiss stage, where the alleged facts in the complaint must be accepted as true. Second, unlike *Ramirez*, claims in privacy and cyber litigation are often premised on the common law torts instead of or in addition to statutory violations. Third, plaintiffs in privacy and cyber class actions typically allege that their injury includes the risk of a future harm, which implicates the Second Circuit's decision in *McMorris v. Carlos Lopez & Associates, LLC.*[3] Significantly, courts have continued to use some form of the metric established by *McMorris*, even after *Ramirez*. Thus, defendants should consider standing from the *McMorris* point of view, regardless of jurisdiction.

1. Courts have distinguished recent data breach cases from *Ramirez* based on the procedural posture of the cases and the types of claims at issue.

One of the first cases to analyze standing in the context of a data breach after the Ramirez decision was *In re Blackbaud, Inc., Customer Data Breach Litigation*,[4] which involved a consolidated class action complaint following a purported data breach.[5] The defendant filed a motion to dismiss for lack for subject matter arguing that plaintiffs lacked Article III standing to pursue their claims.[6] The district court disagreed, finding that the complaint sufficiently alleged that the breach of the defendant's systems resulted in the plaintiff's alleged injuries.[7] The district court further noted that, even if the defendant had challenged Article III standing based on lack of concrete injury, the *Ramirez* decision would not change the analysis because it did not have the "helpful benefit of a jury verdict," unlike in *Ramirez*.[8]

Similarly, other district courts have found that general allegations of harm resulting from the past disclosure of

private information are sufficient to survive an early motion to dismiss. For example, in *In re GE/CBPS Data Breach Litigation*, the district court determined that a constitutional standing analysis is not proper at such an early stage of the litigation. Instead, the district court found that "[p]laintiff has made a sufficient showing at this stage of the litigation to establish his standing under Article III, based on the circumstances of the Data Breach, the allegations regarding misuse of PII exposed in the Data Breach, and the potential uses of the PII to target Plaintiff and other class members for identity theft or fraud."[9]

A few district courts have cited *Ramirez* as support for dismissing data breach and privacy claims at the pleadings stage. For example, in *I.C. v. Zynga, Inc.*, the district court granted a motion to dismiss, finding that plaintiffs failed to sufficiently allege an invasion of privacy or risk of future harm claim.[10] But it is worth noting that the *Zynga* court also granted plaintiffs leave to amend the complaint, and specifically provided guidance regarding the type of allegations needed to state a claim for invasion of privacy, including facts supporting the "risk of identity theft" and "credible threats of real and immediate harm" stemming from theft of private information.[11]

2. *Ramirez* may have a limited impact on those cases that involve non-statutory [or common law] types of claims.

The vast majority of cases after *Ramirez* have asserted similar statutory claims that a court must then analogize to a common law tort in order to determine whether a concrete injury exists such to confer Article III standing. These cases have not been privacy or data breach matters. Instead, for instance, there have been many class actions filed that assert violations of the Fair Credit Reporting Act or the Fair Debt Collection Practices Act. Those plaintiffs may have a more difficult time overcoming a standing challenge in a post-*Ramirez* world.

However, in privacy and data breach cases, courts have found that *Ramirez* is distinguishable because of the type of injury alleged. For instance, in *Mastel v. Miniclip SA*, the district court found that *Ramirez* "involved a fundamentally different type of injury," *i.e.* a statutory violation that was analogized to the tort of defamation – which requires dissemination of the offending material.[12] The *Mastel* plaintiffs, on the other hand, asserted an invasion of privacy claim under the California Constitution, which was akin to other invasion of privacy torts, like intrusion upon seclusion. Notably, the district court specifically stated that similar cases, like *In re Facebook, Inc. Internet Tracking Litigation*[13] and *Eichenberger v. ESPN, Inc.*,[14] were not overruled by *Ramirez* and were more on point because, unlike the tort of defamation at issue in *Ramirez*, "the invasion [of privacy] itself causes harm to the plaintiff's interest in controlling the information" and does not require a separate showing of publication.[15]

Moreover, in *Griffey v. Magellan Health Incorporated*, the district court noted that Ramirez actually recognized that the disclosure of private information is an intangible harm that satisfies Article III standing.[16]

3. *Ramirez* has the greatest impact in cases with threadbare allegations.

Courts have dismissed privacy claims for lack of Article III standing based on the failure to meet basic pleading requirements – rather than a general finding that the plaintiffs did not suffer a concrete harm. In *King v. Peoplenet*, the district court cited *Ramirez* for the proposition that "[t]he requirements of standing guarantee that the plaintiff has a 'personal stake' in the litigation" and found that a plaintiff alleging violation of the Illinois Biometric Information Privacy Act failed to establish Article III standing when the plaintiff's claim was based on the defendant's failure to publish a policy regarding its retention of biometric data – not its unlawful retention of her

data – and she failed to allege how she suffered an injury-in-fact as a result of the defendant's failure to publish a policy.[17]

Likewise, in *Saleh v. Nike, Inc.*, the district court noted *Ramirez*'s "no concrete harm, no standing" conclusion and found that a plaintiff failed to establish Article III standing to assert a wiretapping claim against Nike with regard to its inclusion of a third party's tracking software on its website. The complaint did not allege any concrete injury resulting from Nike's mere possession of the third party's software because "possession does not lead to actual injury, but only potential injury, which is insufficient under Article III."[18]

4. The *McMorris* factors may better identify risk of future harm sufficient for standing.

Courts continue to consider allegations of the risk of future harm, despite the fact that the Supreme Court indicated that such claims could only serve to support a claim for injunctive relief in *Ramirez*. This may be due to the different procedural posture of most data breach and privacy cases, as opposed to *Ramirez*. However, it is probably also a recognition that *Ramirez* is simply not a data breach case.

In *Cotter v. Checkers Drive-In Restaurants*, the district court expressly found that a data breach case that was in the "early pleadings stages" in which the plaintiffs sought compensatory damages (and not just statutory damages) was "outside of [*Ramirez*'s] reach" and applied the *McMorris* factors[19] in finding Article III standing based on a risk of future harm and approved a class settlement resolving claims resulting from a malware attack.[20]

In *Quintero v. Metro Santurce, Inc*., the district court found that there was no standing where the plaintiffs alleged that there was a ransomware attack, but could not identify any misuse of their PII and failed to allege that they suffered a separate concrete harm due to that attack.[21] Likewise, in *Legg v. Leaders Life Insurance Company*, the district court found that the general description of the risks of identity theft following a data breach, without any specific allegations of the misuse of the relevant data, did not support a finding of concrete injury.[22] While the district courts held that the plaintiffs did not have standing in both cases, it is notable that the decisions were based on factual deficiencies, and not because of any finding in Ramirez.

In *In Re: American Medical Collection Agency, Inc. Customer Data Security Breach Litigation*, the district court found the plaintiffs who incurred expenses to prevent future identity theft upon receipt of a data breach notice did not establish standing because they did not allege that their personal information was actually accessed, stolen, or misused.[23] Conversely, other plaintiffs who claimed that their information was wrongfully assessed and distributed (including those who had unauthorized charges placed on their accounts) did plead a particularized harm because they actually alleged that their personal information was wrongfully accessed and/or misused.[24]

5. How can the cases post-Ramirez help inform future litigation?

Ramirez may not be the impenetrable gatekeeper that some were expecting (or hoping) with regard to data breach and privacy cases, especially if the matters assert non-statutory claims. In those cases, which typically involve claims of future or potential harm, federal courts recently have been inclined to confer standing at the pleading stage when the complaint alleges that the plaintiff's personal information was actually accessed and/or misused.

Of course, that is not to say that Article III standing (and lack of damages generally) cannot be challenged in such cases. Some district courts have dismissed data breach cases post-Ramirez where the plaintiffs did not allege facts demonstrating that their personal information was actually accessed in the breach. However, where access and/or misuse of personal information are alleged in the complaint, it may be useful to consider the *McMorris* factors in addition to the *Ramirez* decision.

Where a complaint sufficiently pleads Article III standing, the legal sufficiency of the alleged harm can still be challenged on an evidence-based motion such as a motion for summary judgment or motion to dismiss for lack of subject matter jurisdiction. Thus, defendants should consider conducting tailored discovery on damages at the outset of the litigation and file an appropriate dispositive motion once such discovery is completed.

Finally, the use of reasonable cybersecurity measures and compliance with recognized security and privacy protocols is always an important and useful factual defense to a plaintiff's claims. Entities are encouraged to devote appropriate human and financial resources to compliance, to conduct regular risk assessments, develop a cybersecurity program (preferably one that complies with one of the nationally recognized security standards, including state-specific requirements), and then implement, refresh, and comply with that program.

Conclusion

While the *Ramirez* decision may not help avoid all privacy and data breach class actions, particularly while these cases are still at the pleading stage, defendants still have sufficient arrows in their quiver. Defendants may defeat claims where the plaintiffs do not allege that their personal information was actually accessed or misused and/or where they otherwise failed to plead a cause of action based on the defendant's actual conduct. Defendants can also defeat such claims if they can establish through evidence that the plaintiff did not suffer damages resulting from their conduct. And as always, the best defense is a good offense and one of the strongest ways to get ahead of (and defeat) data breach and privacy claims is to establish and comply with appropriate privacy practices and reasonable security protocols.

[1] 141 S.Ct. 2190 (June 25, 2021).

[2] This article addresses the trend in federal court cases, and therefore does not discuss state court cases that may reference *Ramirez*.

[3] *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021).

[4] Case No.: 3:20-mn-02972-JMC, 2021 WL 2718439 (S. Car. Jul. 1, 2021)

[5] *Id*. at *3.

[6] It is worth noting that Blackbaud did not contest that the plaintiffs alleged a concrete harm as a result of the purported breach– but instead argued that plaintiffs could not establish that any such harm was traceable to Blackbaud's conduct. *Id*. at *5.

[7] *Id*. at *9.

[8] *Id*. at fn. 15 (quoting *Ramirez*, 141 S.Ct. at 2222 (Thomas, J., dissenting)).

[9] 2021 WL 3406374 (S.D.N.Y. Aug. 4, 2021).

[10] 2021 WL 3271187, *2 (N.D. Cal. July 30, 2021).

[11] *Id*. (quoting *In re Zappos.com, Inc*., 888 F.3d 1020, 1023 (2018) and *Krottner v. Starbucks Corp*., 628 F.3d 1139, [1] 1140, 1143 (9th Cir. 2010)).

[13] 956 F.3d 589 (9th Cir. 2020).
[14] 876 F.3d 979 (9th Cir. 2017).

[15] *Mastel*, 2021 WL 2983198 at *6.

[16] 2021 WL 4427065, *3 (D. Ariz. Sept. 27, 2021).

[17] Case No. 21 CV 27742, 2021 WL 5006692 *3-4 (N.D. Ill. Oct. 28, 2021).

[18] —F.Supp.3d —-2021 WL 4437734, *13 (C.D. Cal. Sept. 27, 2021) (citing *Ramirez*, 141 S. Ct. at 2204).

[19] The Second Circuit determined in the *McMorris* decision April 2021 that plaintiffs can establish injury in fact under an increased risk theory – provided the plaintiffs can

any portion of the [compromised] dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. *McMorris*, 995 F.3d 295 (2d Cir. 2021).

[20] No: 8:19-cv-1386-VMC-CPT, 2021 WL 3773414, *4-6 (M.D. Fla. Aug. 25, 2021).

[21] Case No. 20-01075-WGY (D. Puerto Rico Dec. 9, 2021).

[22] *Id*. at *6.

[23] Case No. CV 19-MD-2904, 2021 WL 5937742, at *10-11 (D. N.J. Dec. 16, 2021).

[24] *Id*. at *7-10.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber