More Stringent Limits

The Future of Data Breach Class Actions After *TransUnion v. Ramirez*

By Matthew D. Berkowitz and Brian M. O'Shea

While data breach class actions will likely remain difficult, complicated, expensive, and uncertain, *Ramirez* may be a vital resource to limit both the size of the lawsuit and potential damages.

On a quiet Friday afternoon at the office, you receive a call from one of your clients. The client tells you his company just learned it has been hacked. You learn that your client does not believe any customer information has been stolen, or if it has, it is not going to be used in any way. He assures you that the situation appears to be under control. It appears that the hacker was just snooping around and that he or she probably did not take any private information. No harm, no foul. But then your client begins to ask you difficult questions: Even though it appears no information was taken, are we facing potential liability in a class action lawsuit? And if the answer is yes, and no one knows about it, do we need to report this data breach incident to our customers? The answers and ramifications may be more complicated than they appear.

Prevalence and Financial Effect of Data Breaches and Data Breach Class Actions

Each year in the United States, there are thousands of data breaches exposing millions of private records. The average cost of a data breach is nearly $4 million—and rising. A "mega breach" of one to ten million records costs $50 million on average, an increase of nearly twenty-five percent since 2018. These sums do not even include the cost of the often unmeasurable harm to a company's reputation for its failure to protect its customers' data.

■ Matthew D. Berkowitz, a partner of Carr Maloney PC in Washington, D.C., is an experienced civil litigator with significant class action experience who represents businesses and professionals in complex disputes. At the trial and appellate levels, he has successfully defended clients in shareholder derivative suits, trademark infringement claims, breach of contract, and negligence suits. Brian O'Shea is an associate of Carr Maloney PC in Washington, D.C., where his practice includes the representation of small, medium, and large businesses whose operations could expose them to significant liability. He also has extensive experience defending clients in class actions, professional liability, and other similar complex business disputes.

As the danger of data breaches increases, data breach class action lawsuits have proliferated. These cases are often large, complex, and difficult to defend. They routinely cost businesses millions in judgments, settlements, and legal fees. Indeed, the cost of even a small data breach may be crippling for a business—and that is before litigation. How can businesses protect themselves from a potential financial catastrophe where there is a data breach but where it appears that there is no misuse, or little misuse, of information? Recently, the United States Supreme Court may have thrown a lifeline to businesses facing such a scenario.

Analysis of Supreme Court's *TransUnion v. Ramirez* Decision

In *TransUnion v. Ramirez*, 141 S. Ct. 2190 (2021), the Supreme Court placed an important limitation on which individuals may potentially participate in a class action lawsuit. The Court held that to participate in a class action and recover damages, all class members must have Article III standing to participate in the case. Put differently, class members must have suffered a "concrete harm" or injury-in-fact to participate in the class action and recover damages.

Ramirez was the first time since 2016 that the Supreme Court examined the issue of standing in connection with a class action lawsuit, when the Court held in the landmark case of *Spokeo, Inc. v. Robbins*, 136 S. Ct. 1540 (2016), that a plaintiff or class representative who allegedly suffered mere statutory violations alone, without anything more, lacked standing to sue. In other words, a plaintiff who suffered a statutory violation did not suffer an actual, concrete injury, or injury-in-fact, sufficient to confer standing.

In *Ramirez*, a class of 8,185 individuals sued TransUnion, a credit reporting agency, under the Fair Credit Reporting Act (FCRA). Ramirez alleged that Tran-

sUnion failed to use reasonable procedures to ensure the accuracy of class members' credit files when the credit reports of Ramirez and the class members indicated that their names showed up on a "terrorist list." However, of the 8,185 class members, the reports of only 1,853 members were transmitted to third parties. The remaining 6,332 reports were never disseminated to any third party—meaning these individuals likely never learned of the error. While the Court ruled that the 1,853 class members whose reports were disseminated to third parties had standing, the remaining class members did not. As the Court stated, "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." Put more simply, if a tree falls in a forest and no one is there, it *does not* make a sound. No harm, no foul. The Court further ruled that the risk of future harm, meaning that an inaccurate credit report may or will be disseminated later, is not a concrete injury. In the end, the Court determined that much of the class in *Ramirez* lacked standing.

While *Ramirez* may limit the ability to file a lawsuit, that does not necessarily eliminate an obligation to report. Several states have mandatory data breach reporting laws, regardless of any actual misuse.

Ramirez is a significant case for the defense of class actions in that it significantly limits the potential exposure that a business may face from a class action lawsuit—especially class actions involving technical statutory violations. In other words, in an FCRA class action, the plaintiffs must not only show that the defendant created an inaccurate or faulty credit report, but also that the plaintiffs suffered from an additional consequence caused by the credit report—such as not being able to borrow money to purchase a house or a vehicle. After *Ramirez*, a risk of future harm may still be sufficient to confer standing, but the risk must be imminent or immediate. An inaccurate credit report, by itself and without nothing more, is insufficient to confer standing.

Potential Effect of *Ramirez* on Data Breach Class Actions

The Supreme Court's holding that all class members must suffer a concrete injury may have an impact well beyond the FCRA. One such area may be data breach class actions. In fact, *Ramirez* and the limits on standing in federal court are already affecting how lower courts are adjudicating these cases. For example, in *I.C. v. Zynga*, Case No. 20-cv-01539-YGR, 2021 U.S. Dist. LEXIS 142907 (N.D. Cal. July 30, 2021), after the defendants moved to dismiss a data breach class action, in part, for lack of standing, the plaintiffs argued they had standing because they suffered a concrete injury. The plaintiffs argued that their personal information was stolen in the data breach, the defendant admitted their personal information was stolen, and that, as a result, they were at substantial risk of identity theft and other future harm. However, the court sided with the defendants and granted the motion to dismiss. The court, citing *Ramirez*, ruled that the plaintiffs failed to allege sufficient facts to show that the specific information that was stolen put the plaintiffs at immediate substantial risk of future identity theft. *Id.* at 5–6. Therefore, the plaintiffs lacked standing. Another example is *McCray v. Wetzel*, Civil Action No. 3:20-cv-139, 2021 U.S. Dist. LEXIS 73782 (W.D.P.A., Apr. 16, 2021) where, just days before the Supreme Court decided *Ramirez*, the court held that the plaintiffs' allegation that they were at increased risk of identity theft and sustained emotional distress, mental anguish, and sleeplessness was insufficient to confer Article III standing in a data breach class action.

In contrast, in *In re GE/CBPS Data Breach Litig.*, Case No. 20-cv-2903-KPF, 2021 U.S. Dist. LEXIS 146020 (S.D.N.Y. Aug. 4, 2021), a case stemming from a phishing attack, the court denied the defendants' motion to dismiss for lack of standing. The court rejected the defendant's argument that the plaintiffs lacked standing because they had not yet suffered a concrete harm because of the breach. Rather, the court ruled that the plaintiffs had standing because they pled sufficient facts to show that the phishing attack was targeted at the plaintiffs' information, that the plaintiffs had already received targeted phishing messages to their personal emails and phone numbers, and that some of the plaintiffs had already suffered identity theft, fraud, and abuse. *Id.* at *14–15. The combination of all these factors meant that the plaintiffs had standing to sue.

The Future of Data Breach Class Actions After *Ramirez*

As these cases show, it appears that *Ramirez* and the more stringent limits placed on Article III standing may have substantially changed the data breach class action environment. Now, to have standing to sue for a data breach, the plaintiffs must allege sufficient facts to show that their personal information has been misused as a result of the breach or, at the very least, the type of information that was taken puts them at substantial risk of future harm (like identity theft). As may be the case with FCRA class actions, the legacy of *Ramirez* may be to substantially limit the number of potential plaintiffs who are eligible to participate in a data breach class action.

However, you still need to answer your client's question as to whether the data breach should be reported when the business does not believe that the information has or will be misused. Does a business need to report a data breach to its customers when it reasonably believes no information was misused? While *Ramirez* may limit the ability to file a lawsuit, that does not necessarily eliminate an obligation to report. Several states have mandatory data breach reporting laws, regardless of any actual misuse. Moreover, while there is currently no federal data breach reporting requirement, this may be changing soon. Therefore, a business may be obligated to report a data breach to the authorities and alert its customers of the breach even when there is no misuse of information.

Ironically, though, a business that acts ethically and complies with reporting requirements may actually be opening itself to a lawsuit by providing customers

with standing to sue. By publicly reporting a data breach, customers could conceivably allege that they suffered emotional harm when they learned from the business (or on the news) that their information may have been stolen.

Therefore, the best answer to your client's difficult Friday afternoon question of whether it must report a breach of its data may be as follows: The best course of action may be to report the breach. Even though it is unlikely that information has been or will be misused, many states have mandatory data breach reporting requirements, regardless of whether information was taken or misused. Although customers will learn that a breach occurred, this, by itself, does not necessarily mean that they will have standing to sue. They likely will have to show that the information taken was in fact misused and that they suffered actual harm as a result. This may be difficult. For example, in the recent case, *McCray v. Wetzel*, Civil Action No. 3:20-cv-139, 2021 U.S. Dist. LEXIS 73782 (W.D.P.A., Apr. 16, 2021), the court considered this exact issue and ruled that an increased risk of identity theft and allegations that the plaintiffs suffered emotional distress as a result of the data breach was insufficient to confer standing. The court dismissed the case because the plaintiffs did not sufficiently allege that they sustained an actual injury as a consequence of the breach.

Defending a data breach class action has been, and will probably continue to be, difficult, complicated, expensive, and uncertain. However, *Ramirez* may ultimately prove to be a vital resource for anyone faced with a data breach class action to limit both the size of the lawsuit and potential damage as well.