USING ARBITRATION AGREEMENTS TO AVOID CLASS ACTION CLAIMS IN DATA BREACH LAWSUITS

Author
Brad C. Moody

May 18, 2018

Baker Donelson's Data Protection, Privacy and Cybersecurity attorneys are pleased to continue a series of client alerts that address significant cyber-threats to your business and discuss ways you can protect your business with thoughtful and timely planning before an emergency arises. Proper planning includes recognition of the threats, assessment of the risk, and then examination of the facts and tools at your disposal to mitigate the risks. The series will address your options, from adopting appropriate IT policies and procedures to acquiring contractual indemnity and insurance for specific loss risks. When there is a recommended technical solution available, we will consult with leading expert vendors and provide their input. We often hear that in today's tech environment, it's not a matter of whether you will be hacked or attacked, but when; therefore, we want to help you be well prepared for future challenges.

Our series will help you get ahead of the game. We offer guidance on shopping for cybersecurity insurance; protecting your business from DDoS attacks (Distributed Denial-of-Service attacks) and ransomware; establishing a smart data management plan; evaluating vendor relationships; handling disgruntled employees and other internal threats; and testing for data security events.

Until recently, a majority of class action lawsuits arising from data breaches have been dismissed early in the proceedings because plaintiffs could not prove they had suffered concrete harm. Courts, however, have started loosening the standards for plaintiffs to establish standing to pursue their claims. As the number of lawsuits increases, businesses need to respond. One option for countering prospective class action claims is the use of arbitration agreements.

Arbitration is favored in the United States. In fact, almost 100 years ago, Congress thought arbitration agreements were important enough to pass the Federal Arbitration Act (FAA) to ensure the enforcement of valid arbitration agreements. Under the FAA, when courts are faced with doubts or ambiguities concerning the scope of an otherwise valid arbitration agreement, those doubts and ambiguities are typically resolved in favor of arbitration. Taking it a step further, courts will enforce arbitration provisions that also prohibit class action claims in arbitration proceedings.

Consider the following example: a bank lends customers money, requiring the execution of loan agreements. The loan agreement contains a valid arbitration clause that pertains to all disputes that relate in any way to the agreement between the parties. The arbitration agreement also includes the following provision: "no party to this arbitration agreement may bring a class action or other action in a representative capacity." Several years later, there is a bank-wide data breach, and the bank's customers' personal information is compromised. The customers file a class action lawsuit against the bank. Under these circumstances, the trial court would dismiss the lawsuit and order the dispute to binding arbitration. Moreover, because the U.S. Supreme Court upheld arbitration provisions prohibiting class claims in arbitration, the arbitrator dismissed all class action claims.
In this hypothetical case, the bank's agreement explicitly prohibited class action claims. Including an explicit prohibition against class claims is the best practice instead of leaving it to a court or arbitrator to determine whether the parties agreed to allow class action claims. For example, in *Varela v. Lamps Plus, Inc.*, a criminal hacked an employer's IT system and stole approximately 1,300 employees' personal information. The employees signed an employment agreement that contained, in pertinent part, the following arbitration clause: "The Company and I mutually consent to the resolution by arbitration of all claims or controversies ("claims"), past, present or future, that I may have against the Company . . . ." The arbitration clause did not, however, contain a prohibition against class arbitration. The employees filed a class action lawsuit against the employer in federal court in California based on the data breach. Although the arbitration agreement was enforced, the arbitration proceeding was ordered to proceed on a class basis.

As a comparison, in *Shore v. Johnson & Bell*, a class of individuals whose personal information was compromised after a data breach sued their lawyers who stored the data. The plaintiffs had signed an engagement letter containing the following clause: "Although we do not expect that any dispute between us will arise, in the unlikely event of any dispute under this agreement, including a dispute regarding the amount of fees or the quality of our services, such dispute shall be determined through binding arbitration." In the *Shore* case, an Illinois district court dismissed the class action claims and sent the litigation to arbitration on an individualized basis – as opposed to a class action. The district court reasoned that "[t]he client engagement letter's arbitration clause does not explicitly or implicitly agree to the use of class arbitration." It may have been merely good fortune that the defendants in *Shore* avoided the class claims.

Companies that store sensitive data should take note of the *Varela* and *Shore* cases. First and foremost, companies should consider having arbitration agreements with consumers (or anyone else) for whom it stores confidential information. If used, the arbitration agreements should contain broad language to cover *any and all* disputes that "relate in any way" to the underlying agreement between the parties. Moreover, the arbitration provision should explicitly state that class arbitration is prohibited. Otherwise, companies will be leaving their fate to the discretion of courts, which may vary in their level of skepticism toward the scope of the parties' agreements.

If you have questions regarding the content of this alert, please contact Brad Moody, CIPP/US or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.