Published on *The National Law Review* https://natlawreview.com

Sonic Data Privacy MDL Headed to Trial? Court Denies Defendant's Motion for Summary Judgment

Article By:

Kristin L. Bryan

We've been following the Sonic cybersecurity MDL for some time now. Just last month the Sixth Circuit rejected Sonic's bid to appeal a federal district court's certification of a class under Fed. R. Civ. P. 23 to recover economic damages incurred by various financial institutions and credit unions arising from their reissuance of cards and reimbursement of accounts following a cyberattack directed at Sonic in 2017. The bad news keeps piling on, as this week the district court overseeing the litigation denied Sonic's motion for summary judgment—putting the case on track to potentially be one of the first data breach cases to go to trial. *In re Sonic Corp. Customer Data Sec. Breach Litig.*, 2021 U.S. Dist. LEXIS 168504 (N.D. Ohio Sep. 7, 2021).

As a recap, in 2017 unidentified third parties accessed Sonic customers' payment card data. The hackers purportedly obtained customer payment card information from more than three-hundred Sonic Drive-Ins. Litigation followed, which was consolidated into multidistrict litigation. In the consolidated MDL complaint, Sonic customers alleged that their personal information had been exposed to criminals and was at risk of future misuse. These claims were eventually settled. However, claims were also filed against Sonic on behalf of various financial institutions—this is the litigation that remains ongoing in the Northern District of Ohio.

The court had previously granted in part Sonic's motion to dismiss—meaning that the only claim still pending in the litigation was for negligence (under Oklahoma law, based on applicable choice of law rules). Under Oklahoma Supreme Court precedent, a negligence claim requires that **(1)** Defendants owed Plaintiffs a duty of care; **(2)** Defendants breached their duty; and **(3)** Defendants' breach caused Plaintiffs' injury.

In seeking summary judgment, Sonic argued that Plaintiffs' claim failed as they could not satisfy the duty and causation elements of a negligence claim. The Court disagreed.

Recall that the standard for summary judgment provides that if "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." A genuine issue of material fact exists only where "a reasonable jury could return a verdict for the nonmoving party" based on the evidence.

Now let's turn to Sonic's arguments on summary judgment.

First, Sonic argued that it did not owe Plaintiffs a duty to prevent the data event at issue. Relying on applicable Oklahoma law, Sonic noted that "except in certain circumstances, Defendants do not have a duty to 'anticipate and prevent the intentional or criminal acts of a third party.'" Based on this precedent, Sonic argued it owed Plaintiffs a duty only if their own *affirmative* conduct "has created or exposed [Plaintiffs] to a recognizable high degree of risk of harm through such misconduct, which a reasonable [person] would have taken into account." Sonic asserted that this standard could not be satisfied, on the basis that "Plaintiffs have not and cannot show that Defendants' affirmative acts created a risk of harm from a data breach." Rather, according to Sonic, the data event at issue involved Sonic's point-of-sale system vendor.

These arguments were not persuasive to the Court, which held that "Sonic's affirmative acts created a risk of harm, and Sonic knew or should have known that the risk of hacking made its flawed security practices unreasonably dangerous." This was because, the Court found, "Sonic required franchisees to use middleware transaction processing software that did not allow end-to-end encryption of payment card data." This resulted in Sonic franchisees "storing unencrypted transaction data on the franchisees' servers" and it was this transaction data that was subsequently targeted and exfiltrated in the 2017 data event.

Second, in regards to the element of causation, Sonic also argued that its actions were not the proximate cause of the data breach. This was because, Sonic asserted, "the hackers' breach and data theft acted as supervening causes that cut off Defendants' liability." Applying the circumstances of the case in the context of applicable Oklahoma law, the Court also rejected this assertion. The Court held that Sonic could only prevail on this argument by showing that: **(1)** "the hackers' criminal acts were independent of Sonic's negligent security practices"; **(2)** "that these criminal acts were adequate of themselves to bring about the hack"; and **(3)** "that the hack was not a reasonably foreseeable event." Unfortunately for Sonic, the Court found that questions of material fact existed as to all three of these issues.

A case status conference has been scheduled for mid-September. In the meantime, all eyes will be on Sonic and how it responds to this latest development. While the litigation involves application of Oklahoma law—which is infrequently litigated in data privacy disputes—the key issues implicated by the case (such as breaches caused by vendors and the intersection between cybersecurity considerations and the supply chain) are of broader interest. Stay tuned-CPW will be there to keep you in the loop.

National Law Review, Volume XI, Number 253