Significant data breach class action ruling

James J. Giszczak, Dominic A. Paluzzi | Friday, January 30, 2015

In the first data breach class action of its kind in Michigan, the Court of Appeals has held that a plaintiff must show that the defendant intended to publicly disclose private facts in order for a claim of invasion of privacy to prove successful. In *Jane Doe v Henry Ford Health System*, Nos. 317973, 317975, Wayne County Circuit Court Case No. 12-001649-NO, a patient of Henry Ford filed a class action lawsuit against the health system and its transcription service providers after the service provider changed a configuration on the Henry Ford server resulting in hundreds of patients' (including the plaintiff's) protected health information (PHI) being made publicly available through search engines on the Internet.

Background facts

The patients' names, medical record numbers, dates of patients' visits, locations of the visits, physicians' names, and summaries of the visits were viewable online. In the anonymous plaintiff's case, this information included diagnoses of "Cervical dysplasia secondary to HPV (Human Papillomavirus)" – a sexually transmitted disease. After Henry Ford learned of the issue, all PHI was removed from the Internet, affected patients were provided with written notification, and steps were taken to more adequately protect PHI. The Court of Appeals stated, "there is no indication in the lower court record that the information in question was viewed by a third party on the Internet or that it was used inappropriately . . . . Plaintiff likewise conceded at her deposition that she had no indication that anyone saw, or used, any of her information that had been made visible on the Internet."

After receiving notification of the breach, plaintiff filed a lawsuit in Wayne County Circuit Court and sought class certification. Her complaint had three claims: (1) negligence; (2) invasion of privacy; and (3) breach of contract. Although plaintiff sought “all damages”, when pressed on the issue in discovery, she advanced a theory of “presumed damages”. The only losses, however, that plaintiff allegedly incurred was $275 for LifeLock credit monitoring.

Despite objections from defendants Henry Ford and Perry Johnson and Associates, Inc., the trial court granted class certification for 159 similarly situated plaintiffs and denied defendants’ motions for summary disposition. Defendants appealed both rulings and were granted leave.

Court of Appeals decision

The three-judge panel said in its decision that summary disposition should have been granted by the trial judge in favor of the defendants and ordered that the action be sent back to the trial judge for that purpose. The Court of Appeals also reversed the class certification.

The appellate court explained that in Michigan an invasion of privacy is based on intention, but in this case the medical records were exposed due to an accidental error by the subcontractor. “We are not aware of a Michigan case to overtly consider whether the disclosure of information to the public must be intentionally done, but nonetheless our review of Michigan caselaw leads us to conclude that it is in fact an intentional tort. Specifically, we find it notable that the public disclosure of private facts has been discussed by the Michigan Supreme Court as an intentional tort,” the Court of Appeals stated.

“Because the undisputed facts in this case indicate nothing more than a negligent disclosure of private information, no material question of fact remains and summary disposition should have been granted regarding plaintiff’s invasion of privacy claim,” the panel wrote.

In addition, the plaintiff’s claims for negligence and breach of contact failed because there was no showing of any actual damages as a result of the unintentional disclosure. The Court held that the “plaintiff’s identity theft protection services are not cognizable damages in the absence of present injury.” The panel indicated that any damages that are incurred in anticipation of possible future injury (such as credit monitoring costs), rather than in response to present injuries, are not cognizable under Michigan law. “Plaintiff has not shown that the costs for the credit monitoring services related to a present, actual injury," the appellate court explained.

Michigan now joins the majority of state courts that have dismissed data breach cases based on a failure to prove actual cognizable damages as a result of the breach. McDonald Hopkins will continue to monitor the status of data breach litigation and provide timely updates.

The McDonald Hopkins' national Data Privacy and Cybersecurity team served as attorneys of record for one of the defendants.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Significant data breach class action ruling

Dominic A. Paluzzi