Goodmans LLP Update

Clarity Emerging in Data Breach Class Actions and the Risks Are High

A recent decision of the Ontario Superior Court suggests that judges are increasingly willing to certify class actions brought in respect of data breaches. That willingness, when combined with the nearly Canada-wide statutory obligations to report privacy breaches whenever there is a "real risk of significant harm", means that companies that suffer a data breach involving sensitive information belonging to a large group of individuals should expect to be the subject of a class action. And judging by the reasons given in *Stewart v. Demme*, a class action is likely to be certified if the type of sensitive information accessed is the same for all affected individuals. In the interests of avoiding the significant costs of defending class proceedings (not to mention the liability risk), organizations would be well-advised to devote additional resources to improving privacy protection.

Background

Class actions involving data breaches typically include a relatively novel cause of action known as "intrusion upon seclusion", which was recognized by the Ontario Court of Appeal eight years ago in *Jones v. Tsige*. The Court of Appeal adopted a three-part test to establish the cause of action:

1. the defendant wilfully or recklessly intruded upon the plaintiff's affairs;
2. the affairs intruded upon were private; and
3. the intrusion would be viewed as offensive to the reasonable person, causing distress, humiliation or anguish.

Left unclear, however, was whether the plaintiff needed to show that the intrusion had actually caused distress, humiliation or anguish, or whether such mental suffering would be presumed.

This lack of clarity, as well as the relative novelty of the cause of action, resulted in a high degree of uncertainty in data breach class actions, almost all of which plead the tort of intrusion upon seclusion. However, recent decisions, of which *Stewart v. Demme* is the latest, suggest that certification is very likely where the type of data accessed is sensitive and is uniform across the plaintiff class.

Stewart v. Demme

This class action has been brought on behalf of 11,000 persons whose health records were accessed without authorization by an employee of a Toronto-area hospital. The employee used her access to the health records in order to obtain narcotics for her own personal use from the hospital's dispensing system. The access to the plaintiffs' health records was "fleeting" – typically lasting less than 60 seconds in each case. No one was harmed as a result of the employee's actions. In addition, no copies were made of the information, nor was the information shared with any other person, nor was there any suggestion that the employee could remember any of the details of the information that she reviewed.

Nevertheless, the motions judge certified the class action. The Court held the intrusion was "its own harm", and that any intrusion – even a very small one – into highly sensitive information, such as health records, is "highly offensive" and therefore actionable. The Court seemed to proceed on the basis that, because of the highly

Authors

Julie Rosenthal
jrosenthal@goodmans.ca
416.597.4259

Peter Ruby
pruby@goodmans.ca
416.597.4184

Monique McAlister
mmcalister@goodmans.ca
416.597.4255

sensitive nature of medical records, there was no need for any plaintiff to prove that they had been upset or embarrassed by the employee's actions. As a result, liability could be entirely resolved at the common issues trial, leaving only the question of damages to be determined on an individual basis.

Analysis

With the decision in *Stewart v. Demme*, a trend is beginning to emerge in data breach class actions. If the information accessed is sensitive (health and financial records being the most common examples), and if the type of information accessed is uniform across the plaintiff class, then certification appears likely. By contrast, if there is doubt about the sensitivity of the information and/or if there is variability among the plaintiff class as to the type of information at issue, then certification is less likely.

For example, in *Kaplan v. Casino Rama*, an Ontario court refused to certify a class action brought in respect of a data breach at Casino Rama perpetrated by hackers. The type of information accessed (and then posted online) varied widely from person to person. Some had highly sensitive information publicized, while others did not. The court seemed particularly troubled by this variability and, perhaps as a result, held that it would be necessary for each individual plaintiff to prove that he or she had suffered embarrassment or humiliation as a result of the unauthorized access and disclosure. This need for complex individual inquiries led the court to deny certification.

Similarly, in *Broutzas v. Rouge Valley*, certification was refused for a class action that resulted from hospital employees having improperly accessed patient records, with the patients' contact information then being disclosed to third parties. In its reasons refusing to certify the claim, the court focused on the fact that the information that was actually disclosed to the third parties was not sensitive and further noted that the disclosure had not exposed the plaintiffs to any real risk of loss.

By contrast, certification was granted in *Grossman v. Nissan*, where the information accessed included customers' credit scores. The court underlined the "sameness of the data breach", and the fact that any reasonable person would be "highly offended" by unauthorized access to one's credit scores.

For the moment, businesses that are responsible for safeguarding third parties' sensitive personal information, for example, health records, banking information, or credit history, would be prudent to assume that any unauthorized access to that information is likely to lead to a class action, with a high risk of certification being granted. Moreover, even though the quantum of damages potentially payable to each individual would likely be quite small, the total amount payable in a class action could be significant, given the very large number of individuals who are typically affected by data breaches.

Businesses should optimize their privacy protection measures, in the interests of avoiding the significant risks and costs associated with data breach class actions.

For further information about this emerging trend, please contact any member of our Class Actions Group.