Goodmans LLP Update

# Hurdles to Certifying a Cyber-Attack Class Action

A recent decision from the Ontario Superior Court of Justice highlights some of the difficulties plaintiffs might face when seeking to certify a class action relating to the disclosure of personal information from a cyber-attack. Specifically, this case highlights the difficulties in finding commonality in privacy breach cases where the sensitivity of the information stolen is not the same amongst all class members.

## Background

*Kaplan v. Casino Rama* concerns the certification of a proposed class proceeding relating to the cyber-attack of Casino Rama's computer systems in November 2016. An anonymous hacker accessed Casino Rama's computer system, stole personal information of approximately 11,000 customers, employees and suppliers and posted the stolen data online. There was no evidence before the Court that anyone had experienced fraud or identity theft as a result of the cyber-attack, or that anyone had sustained any compensable financial or psychological loss, although they may have been upset about their personal information having been accessed and publicly disclosed. A proposed class proceeding was commenced against Casino Rama (in addition to the Ontario Lottery and Gaming Corporation and various other corporate entities) on behalf of all persons whose personal information was posted online or whose personal information was on servers that were accessed by the hackers. The plaintiffs asserted five causes of action in the claim: negligence, breach of contract, intrusion upon seclusion, breach of confidence and "publicity given to private life".

## Decision

The Court dismissed the plaintiffs' motion for certification and in so doing, highlighted potential difficulties in finding commonality among class members whose private information had been accessed or publicly disclosed in a cyber-attack.

Section 5(1)(c) of the *Class Proceedings Act* requires that claims of the class members raise common issues. For an issue to be common, it must be capable of being answered for all class members. In respect of the plaintiffs' negligence claim, the Court found that because the scope and content of the applicable duty and standard of care depends on the sensitivity of the personal information, there could be no common issues regarding the duty and standard of care. "[T]he less sensitive the information – such as simply one's name and mailing or email address, the lower the duty or standard of care; the more sensitive the information – credit card details, banking information or, say, medical records – the higher the duty and standard of care." In *Kaplan*, the nature of the personal information stolen by the hackers varied widely among the class members. Some of the stolen personal information was private and confidential, but most of it was contact information (which is generally not considered to be private or confidential) and was made up of incomplete information fragments. Any determination of whether the defendants met the standard of care by establishing appropriate security safeguards would necessarily depend on the type and amount of personal information at issue. Given the degree of variance in the personal information stolen, the Court held that liability for negligence could only be determined on an individual class member basis and would overwhelm any common issues.

The Court had similar difficulties with the common issues related to the claim for intrusion upon seclusion, which is based upon the willful or reckless invasion of the privacy of class members in a manner that would be highly offensive to a reasonable person. There was no way to determine, on a class-wide basis, whether all class members' privacy was invaded or whether such invasion would be highly offensive to a reasonable person since that inquiry, again, depends on whether any given class member had private information disclosed or simply personal information.

(Interestingly, the Court also dismissed the claim for breach of confidence. That cause of action requires that the defendants "misuse" confidential information. Here, however, it was the hacker, not the defendants, who misused the class members' personal information.)

For further information on this case or class actions relating to privacy breaches, please contact any member of our Litigation Group.

## Authors

Melanie Ouanounou
mouanounou@goodmans.ca
416.849.6919

Peter Ruby
pruby@goodmans.ca
416.597.4184