Alert

April 11, 2023

COZEN O'CONNOR

No Action for Theft of Personal Information Without Loss

Theft of personal information does not by itself entitle the victim to damages in Canada; proof of loss or harm is required, the Alberta Court of Appeal held recently in *Setoguchi v Uber BV*. This, and other recent decisions, demonstrate that plaintiffs cannot easily win large awards in data breach class actions. This is good news for firms that suffer data breaches. But firms still need robust cybersecurity safeguards to lessen their chances of being hacked, as data breaches have other costly consequences.

Theft of Personal Information from Uber Leads to Class Action

In 2016, rideshare company Uber suffered a data breach. Hackers stole the personal information of about 57 million Uber drivers and customers. The stolen information consisted of names, phone numbers, and email addresses (as well as some U.S. driver's license numbers). Uber paid the hackers a $100,000 ransom to destroy this data.

After the breach became public, Setoguchi, an Uber customer, commenced a class action.

The Alberta Court of King's Bench refused to certify the class. It found that a class action would not be the preferable procedure to resolve the common issues because the only damages that might be common to the class would be nominal and *de minimis*.

Setoguchi appealed.

Inherent Value of Personal Information Cannot Ground a Negligence Claim

The appeal court also focused on the plaintiff's theory of loss. This was important as loss was an essential element of the plaintiff's negligence claim.

The plaintiff had pleaded that class members suffered loss, but it is not enough merely to state that loss was suffered, the court noted. Rather, "a plaintiff is required to plead facts sufficient to amount *at law* to damage."

The plaintiff argued that the action should be certified on the basis of the "first loss." This first loss arises because personal information has inherent value. Its theft thus gives rise to a loss that is common to the class. The plaintiff seems to have adopted this approach in order to get around the problem that there was no evidence of any consequential loss or harm to the class. Even if there were consequential losses, they likely could not be proven on a class-wide basis, but would instead require individual inquiries.

The appeal court rejected this first loss theory. "A claim for either nominal or symbolic damages cannot ground a claim in negligence," the court held. Though the theft of "publicly available information" might make class members "marginally 'worse off,'" this loss is negligible or trivial and not real. It does not "rise above the ordinary annoyances, anxieties, and fears that people living in society routinely accept," as the Supreme Court put it in *Mustapha v Culligan of Canada Ltd.*

As a result, the court held that the negligence claim did not disclose a cause of action.

Class Actions Not Preferable Procedure for Nominal Damages Claims

While the plaintiff's breach of contract claim did not require proof of loss, they would only be entitled to nominal damages in a "trivial" amount. Because of this, a class action would not be the preferable procedure for resolving the breach of contract claims. It would not improve access to justice to certify a case that seems "hopeless for recovery of actual losses."

Michael Osborne

Chair, Canadian Competition Practice

mosborne@cozen.com
Phone: (647) 417-5336
Fax: (416) 361-1405

Related Practice Areas

- Antitrust & Competition
- Technology, Privacy & Data Security

Judicial Skepticism in Data Breach Cases?

The *Uber* case is remarkably similar to the 2021 decision of the Quebec Superior Court in a proposed class action against the Investment Industry Regulatory Organization of Canada (IIROC). An IIROC employee had left an unencrypted laptop containing sensitive information of about 50,000 investors on a train. There was no evidence of any actual misuse of this data. In two separate class actions, one started by Sofio, and the other, by Lamoureux, the Quebec court held that stress suffered by class members did not amount to compensable injury; as in *Uber*, it did not rise "above the ordinary annoyances, anxieties, and fears that people living in society routinely, if sometimes reluctantly, accept." The Quebec Court of Appeal dismissed appeals in both cases.

Uber also follows on the heels of the Ontario Court of Appeal's refusal, in late 2022, to extend liability for the tort of intrusion upon seclusion to defendants that have been hacked by third parties. That case, *Owsianik v. Equifax Canada Co.*, arose as a result of a 2017 hack of personal information stored by Equifax, a credit reporting service. The plaintiffs contended that Equifax was liable for the tort of intrusion upon seclusion because it failed to take appropriate steps to safeguard sensitive financial information it stored.

The tort of intrusion upon seclusion is an intentional tort, however. One of its essential elements is that the *defendant* must have unlawfully invaded or intruded upon the plaintiff's private affairs or concerns. It was the hackers, not Equifax, that had invaded the plaintiff's privacy. "There is simply no conduct capable of amounting to an intrusion into, or an invasion of, the plaintiff's privacy alleged against Equifax in the claim." Negligent storage of information cannot amount to an intrusion, the court held.

While these cases suggest judicial skepticism about class actions seeking compensation from firms that are hacked, not all defendants have met with equal success. For example, in *Tucci v. Peoples Trust Company,* the British Columbia Court of Appeal largely upheld a decision to certify a data breach class action arising out of a data breach suffered by Peoples Trust. In that case, the court of appeal seems to have accepted that nominal damages could be "awarded to acknowledge the commission of a legal wrong where no actual loss is proven."

Robust Cybersecurity Safeguards Still Needed

Apart from class action liability, data breaches can trigger large fines and important reputational consequences.

In Canada, as in many other jurisdictions, data breaches that pose a real risk of harm to individuals must be reported to the Office of the Privacy Commissioner. Canada's proposed new Consumer Privacy Protection Act, which is currently before Parliament as Bill C-27, provides for administrative monetary penalties (AMPs) of up to $10 million, or 3% of an organization's gross global revenue, for failures to adequately safeguard personal information. A statutory cause of action will also enable consumers to recover loss or injury caused by breaches of the new law.

Data breaches can potentially also give rise to penalties under Canada's *Competition Act* if, for example, the breach shows that claims made by a firm about its privacy protections were false or misleading.

In an era when it is commonplace for firms to be the victim of data breaches and ransomware attacks, firms must maintain robust safeguards against cyberattacks and have an emergency plan for dealing with the fallout from a successful cyberattack.

To learn more, contact the author or any member of our Technology, Privacy & Data Security group.