Cassels

No Damages for Lost Laptop Data Breach, Quebec Court Finds

April 28, 2021

Investors whose personal information was potentially exposed when a laptop was left on a train did not suffer any loss beyond the normal annoyances that everyone who lives in society routinely experiences and reluctantly accepts, a Quebec judge held in dismissing the first data breach class action to go to trial.

This case, known as Lamoureux v Organisme canadien de réglementation du commerce des valeurs mobilières, offers a number of lessons for organizations that suffer a data breach. Among other things, it shows how a quick and careful response, plus a bit of luck, can help an organization to reduce or entirely avoid large claims for damages.

Lost Laptop Leads to Data Breach

In February 2013, an Investment Industry Regulatory Organization of Canada (IIROC) investigator left a laptop on a train. Although the laptop had password protection, it was unencrypted.

IIROC's response consisted of four elements:

- **Investigation:** IIROC hired computer forensic investigators from Deloitte to investigate the data breach. Deloitte found that the laptop contained sensitive information about more than 50,000 clients of investment firms.
- **Reporting:** IIROC reported the breach to provincial and federal privacy commissioners.
- **Mitigation:** IIROC contracted with Equifax and TransUnion to put in place measures to protect the affected clients, including alerts on their files that their identity may have been compromised.
- **Communication:** IIROC issued a press release in mid- April 2013 and followed up with letters out to affected investors towards the end of the month. IIROC set up a call centre to answer questions.

The Sofio Class Action

A class action was launched within days of IIROC's letter to investors with Paul Sofio as representative plaintiff. The class action sought $1,000 for each investor for the stress and inconvenience occasioned by the breach.

The Quebec court refused to authorize (certify) this class action, however, finding that Sofio had not shown a compensable injury. This finding was upheld by the Quebec Court of Appeal in 2015.

The Lamoureux Class Action

Very shortly after the appeal decision in the *Sofio* class action, a second class action was launched, with Danny Lamoureux as representative plaintiff. Lamoureux provided more details about anxiety and stress he suffered, and the steps he had to take as a result of the data breach. He also alleged that the data breach led to the theft of his identity.

This class action was authorized and proceeded to trial.

No Compensable Injury

As IIROC admitted to a fault (essentially, negligence) in relation to the data breach, the question was whether the plaintiffs had suffered any compensable injury.

Seven class members who testified at trial had experienced anger, worry, and stress, but these sentiments were general in nature; the witnesses provided few concrete details. Nor was there any medical evidence as to the severity of their experience.

As a result, the disturbance suffered by class members did not rise “above the ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept”, as the Supreme Court put it in Mustapha v Culligan of Canada Ltd.; it was not a compensable injury.

Lamoureux also failed to prove that the identity theft he and some other class members suffered was related to the loss of the laptop. IIROC’s experts determined that the information about Lamoureux on the lost laptop did not include either his driver’s licence or social insurance number. The experts also found that there was a lack of commonality that would be expected from a targeted attack on a recovered set of data. Indeed, as the judge noted, it is not known whether personal information was harvested from the laptop by whoever found it.

No Punitive Damages

The judge also rejected the claim for punitive damages. The plaintiffs accused IIROC of being slow to respond to the data breach, pointing to the two months between the loss of the laptop and the first communication to investors.

The judge found no fault with IIROC's response. Indeed, he noted that releasing information to the public too quickly could create a risk that the laptop would be targeted and end up in the wrong hands before protective measures could be put into place.

Data Breach Damages Are Not Inevitable

Many organizations have experienced data breaches, whether as a result of hacking or lost media containing data. Class actions typically follow the public reporting of these breaches.

While class actions may be inevitable after a data breach, paying out large damage awards to plaintiffs is not.

The steps an organization takes to respond and deal with a data breach can help it avoid or minimize its exposure. Organizations that learn of a data breach should follow the same four-step approach taken by IIROC: investigate the breach, report it to the authorities as required, take steps to mitigate the harm to those affected, and communicate with those affected.

As well, this decision signals that courts will require proof of actual compensable injury, not just inconvenience, annoyance, or even anxiety, before awarding damages to plaintiffs. Serious trauma or illness must be proven. Medical evidence will almost certainly be required. While the Quebec court was prepared to assume that the entire class had suffered annoyance on the basis of the testimony of seven witnesses, it is hard to imagine how plaintiffs could prove that everyone in the class suffered sufficiently serious mental trauma so as to have suffered compensable damages.

That said, it remains to be seen whether courts outside of Quebec will impose this rigour on plaintiffs. While negligence-based claims require proof of injury, some common law causes of action that may be available for a data breach do not. For example, nominal damages are available for breach of contract, and moral or symbolic damages are available for the tort of intrusion upon seclusion (in Ontario at least). Even nominal damages could be enormous over a large class, however. Damages for humiliation are available under federal privacy legislation (the *Personal Information Protection and Electronic Documents Act*). The availability of these causes of action will depend upon the facts of the case.

In a recent case in Ontario, the Court refused to certify a proposed class action against Facebook because there was no evidence that users' personal information was shared with Cambridge Analytica. See: Lack of Evidence Dooms Facebook Class Action.

Cassels

This publication is a general summary of the law. It does not replace legal advice tailored to your specific circumstances.