NO DAMAGES FOR MINOR STRESS AND INCONVENIENCE: QUEBEC COURT DISMISSES DATA BREACH CLASS ACTION

Posted on June 9, 2021

Categories: Insights, Publications

In March, the Québec Superior Court released a rare decision in which it dismissed a privacy class action on the merits. *Lamoureux c. OCRCVM*[1] concerned a class action against the Investment Industry Regulatory Organization of Canada ("**IIROC**") for damages arising out of a data breach. In the course of the Court's dismissal of the action, it established a minimum threshold for damages and clarified best practices for organizations when responding to a data breach.

A LOST LAPTOP

The data breach occurred in February of 2013 when an IIROC inspector accidentally forgot a company laptop in the luggage compartment of a train (the "**Laptop Incident**"). The laptop contained the personal information of thousands of Canadian investors. Despite its best efforts, IIROC was not able to recover the laptop.[2]

After the incident, one affected individual, Paul Sofio, brought a class action against IIROC. That class action was dismissed at trial because the judge concluded that Sofio could not establish *prima facie* that he suffered compensable damages under article 1003 of Québec's former Code of Civil Procedure.[3] This judgment was upheld by the Quebec Court of Appeal.[4]

Danny Lamoureux brought a separate class action, seeking compensation for the stress, anxiety, worry, and anger felt by the members of the class, as well as the inconvenience, loss of time and expense caused by the protective measures put in place by IIROC. A subset of the class also sought damages for identity theft, fraud or attempted fraud of which they were victims, alleging a connection between these attacks and the Laptop Incident.

CLASS ACTION DISMISSED

The Court dismissed the action on the basis that:

i. the class could not establish they had suffered compensable damages;
ii. there was no evidentiary support for the allegation that identity theft or fraud suffered by some class members was connected to the Laptop Incident; and

iii. the defendant's behavior following the breach met the standard for a data breach response and therefore there was no intentional wrongdoing worthy of punitive damages.

i. Minor Inconveniences is Not Compensable

The Court held that while the plaintiff class did not have to show actual identity theft in order to have compensable damages, the plaintiff must demonstrate that it suffered more than minor inconveniences.[5] The Court found that the plaintiff class did not meet that threshold, noting a lack of documentary or medical evidence, and concluding that the fears, anxieties, and stress of the class members, as well as delays in obtaining credit, were relatively normal inconveniences that people in society are obliged to accept.[6]

Notably, following discovery of the breach, the defendant provided affected individuals with credit supervision and protection measures from Equifax and TransUnion free of charge. The Court found that the stress and inconvenience of having to set up credit monitoring was too minor to be compensable.[7]

ii. Expert Witness Rebutted Claim

IIROC entered extensive uncontradicted expert evidence showing that the identify theft alleged by some of the class members could not have been connected to the information purportedly stolen from the lost laptop.[8] This evidence showed that the identify theft and fraud alleged by some class members lacked commonality, and in some cases required information that was not available on the laptop.[9] This led the Court to conclude that data involved in these crimes were unrelated to the Laptop Incident.[10]

iii. Punitive Damages is Not Possible without Evidence of Wrongdoing

In Quebec, punitive damages constitute their own cause of action stemming from the conduct of the defendant.[11] Therefore, despite the failure of the class to show they suffered compensable damages connected to the Laptop Incident, the Court considered the possibility of awarding punitive damages in this case, based solely on IIROC's conduct.

The Court refused to award punitive damages, finding that IIROC reacted in accordance with the standards expected of them.[12] The case therefore provides a good overview of the sorts of things a court will expect from an organization responding to a data breach. The measures IIROC took in response to the security threat included:

- initiating a fulsome internal investigation as soon as they became aware of the breach;
- hiring a third party forensic team;
- notifying all appropriate parties, including
    - the Montreal Police Department,

    - the Quebec Commission de l'access du information and the Federal Office of the Privacy Commissioner,
    - brokerage firms with concerned investors, and
    - individuals whose personal information was compromised;
- offering one year of complimentary credit monitoring to affected individuals, among other credit protection measures; and
- issuing a press release explaining the incident.

The Court acknowledged that the company was not perfect in its prevention scheme. IIROC admitted that they failed to ensure maximum protection of members' personal information by encrypting the lost computer.[13] Nevertheless, when it came to their response to the breach, the Court accepted the expert opinion of the defendants that IIROC adhered to best practices.[14]

The plaintiffs' primary basis for alleging punitive damages was IIROC's delay in providing notice. Indeed, IIROC did not notify affected individuals of the breach until over a month after the loss was discovered.[15] Their explanation for the delay was that a certain period of time was necessary to precisely identify the personal information concerned as well as the firms and individuals affected, and put in place measures to ensure upstream protection of information and answer questions arising from the announcement of the incident. They argued that if they had disclosed the information too early, there was a risk that the unidentified computer would be targeted and end up in the wrong hands.

TAKEAWAYS

There are two key takeaways from this decision that we wish to emphasize.

First, the decision helps establish the measure for adequate responses to data breaches. The decision is reminiscent of the 2016 *Lozanski v Home Depot* decision in Ontario.[16] In that case, Home Depot's payment card system was hacked by criminal intruders with custom-built malware, which resulted in unauthorized access to customer information of approximately 500,000 customers. While *Home Depot* was a settlement approval decision, the judge expressed the opinion that Home Depot had done nothing wrong. According to the decision, "Home Depot responded in a responsible, prompt, generous, and exemplary fashion to the criminal acts perpetrated on it by the computer hackers", offering twelve free months of identity protection services, credit monitoring, and credit repair services.[17] The judge even wrote (in obiter) that he would have approved a discontinuance of the settlement without any benefits achieved by the putative class members.[18]

The *Lamoureux c. OCRCVM* case provides an even more reliable stamp of approval than *Home Depot* on the measures carried out by IIROC. However, IIROC's measures should not be treated as a perfect roadmap for every kind of data breach. The best response to a data breach depends on the context. For example, where the

harm to consumers is immediately discernable and data is already in the wrong hands, a court may expect an organization to notify consumers of the potential breach much earlier.

Second, the decision reinforces that minor inconveniences are not compensable in a privacy class action. This may change the outcome of future class action certification decisions similar to *Zuckerman v Target* or *Lévy v Nissan*, in which the inconvenience and time spent carrying out protective measures were included as damages.[19]

[1] *Lamoureux c. OCRCVM*, 2021 QCCS 1093 ("**Lamoureux c OCRCVM**"); OCRCVM stands for Organisme canadien de réglementation du commerce des valeurs mobilières, which is the French name for the Investment Industry Regulatory Organization of Canada ("**IIROC**").
[2] *Lamoureux c. OCRCVM*, para 9.
[3] *Sofio v. Investment Industry Regulatory Organization of Canada (IIROC)*, 2014 QCCS 4061.
[4] *Sofio v Investment Industry Regulatory Organization of Canada (IIROC)*, 2015 QCCA 1820.
[5] *Lamoureux c. OCRCVM*, para 72.
[6] *Lamoureux c. OCRCVM*, paras 68-72.
[7] *Lamoureux c. OCRCVM*, para 85.
[8] *Lamoureux c. OCRCVM*, para 102.
[9] *Lamoureux c. OCRCVM*, paras 105-107, 113-115.
[10] *Lamoureux c. OCRCVM*, para 118.
[11] *Lamoureux c. OCRCVM*, para 120, citing *de Montigny v. Brossard (Succession)*, 2010 SCC 51, para 47.
[12] *Lamoureux c. OCRCVM*, para 134.
[13] The court noted that the laptop was protected by a password, but the data within was not encrypted, even though it was highly sensitive in nature: *Lamoureux c. OCRCVM*, para 10. The Federal Office of the Privacy Commissioner has routinely recommended that sensitive personal information be protected by encryption: see OPC investigation reports on Vtech Holdings Limited; Equifax Inc.; TJX/Winners; WhatsApp; CIBC; Adobe; and the World Anti-Doping database.
[14] *Lamoureux c. OCRCVM*, para 130.
[15] *Lamoureux c. OCRCVM*, paras 9-18. The Laptop Incident occurred on February 22, 2013. Following its internal investigation, IIROC established as of March 4, 2013 that the laptop likely contained information concerning thousands of individuals and legal entities. Despite this, the affected brokerage firms were only informed during in-person meetings on April 8 and 9, 2013, and the first public press release issued on April 11, 2013.
[16] *Lozanski v The Home Depot, Inc.* 2016 ONSC 5447 ("**Home Depot**").
[17] *Home Depot*, para 10.

[18] *Home Depot*, para 74.
[19] *Zuckerman c. Target Corporation*, 2017 QCCS 110, para 73; *Lévy c. Nissan Canada Inc.*, 2019 QCCS 3957, para 104-108 ("**Lévy**").

by Mitch Koczerginski and Robbie Grant

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.