

Superior Court Of Québec Authorizes Privacy Class Action In Zuckerman V. Target Corporation

February 03, 2017

The Superior Court of Québec recently rendered judgment on a motion to authorize a privacy class action in Zuckerman v. Target Corporation.

Privacy class actions triggered by data breaches are growing in popularity in Canada, with more than 30 of them pending throughout the country. While none of these cases have yet been heard on their merits, some are being certified or authorized. In Québec, there are at least seven privacy class actions before the courts.

The Superior Court of Québec recently rendered judgment on a motion to authorize a privacy class action in Zuckerman v. Target Corporation,¹ in which the petitioner alleged damages as a result of a data breach involving an estimated 40 million credit and debit cards, as well as the personal information of up to 70 million customers.

The Nature of the Breach

The motion followed a public acknowledgement by the respondent Target in late 2013 to the effect that there had been unauthorized access to "payment card data" in its U.S. stores, including names, card numbers, expiration dates, and security codes. Target later acknowledged that encrypted PIN data had been removed from its system (while maintaining that PINs were secure), and that customer names, addresses, phone numbers, and email addresses had also been taken.

Target had offered free credit monitoring for a year to all customers (including Canadians) who shopped in its U.S. stores. More than 80 class actions followed in the U.S.; these actions were eventually consolidated into a single proceeding. In Canada, **only the Zuckerman class action was filed.**

Jurisdictional Issues

After a preliminary jurisdictional challenge, Target argued forum non conveniens, alleging that its domicile, witnesses, and evidence were all in Minnesota. The Superior Court found that the same argument could be made from the petitioner's point of view

relative to Québec. It ultimately decided that it would not "force a Quebec resident who has suffered damage as a result of the fault of a large U.S. corporation to sue in Minnesota to recover his damages."² The court also narrowed the proposed class to Québec residents only, based on the specific facts of the case.

Damages Claimed

On behalf of the class, the petitioner alleged damages for fear, confusion, and loss of time (including time spent closely monitoring accounts); costs or fees for credit monitoring services (Mr. Zuckerman had paid \$19.95 for such services prior to Target's offer to provide them free of charge); Target's failure to notify some members of the breach; and potential fraud or identity theft. The petitioner also claimed punitive damages, alleging an intentional breach of class members' privacy.

In contesting the petitioner's ability to make out a prima facie case, Target argued that the inconveniences alleged were not compensable damages; that the expense incurred by the petitioner for credit monitoring was not a direct consequence of the alleged fault (especially in light of Target's offer to pay for such credit monitoring); that the petitioner himself was not the victim of identity theft, fraud, or a failure to notify; and that there was simply no appearance of right with respect to punitive damages.

The question of what counts as compensable damage in privacy class actions has been **the subject of some debate. In Zuckerman, the court recognized that privacy class actions in Québec may be somewhat unpredictable with respect to whether causes of action for inconvenience, stress, and anxiety will be authorized. It acknowledged the Supreme Court's reasons in Mustapha v. Culligan of Canada Ltd.³ to the effect that "psychological disturbance" must be distinguished from mere "psychological upset." It also referred to two Québec class actions, Sofio v. Organisme canadien de réglementation du commerce des valeurs mobilières⁴ and Mazzonna v. DaimlerChrysler Financial Services Canada Inc.⁵ in which the Court of Appeal and Superior Court respectively held that having to make normal or routine financial verifications, while suffering some stress, cannot ground a claim in damages.**

On the other hand, the court also acknowledged statements in Sofio and in another recent case, Belley v. TD Auto Finance,⁶ to the effect that allegations of identity theft are not a necessary condition of authorization in class actions following security breaches.

The court held that while monitoring accounts and credit card statements are normal activities and not inconveniences for which damages can be awarded, activities such as setting up credit monitoring and security alerts, obtaining credit reports, and cancelling or replacing cards and closing accounts are potentially compensable.⁷

Damages Suffered by Other Class Members

The court authorized common questions with respect to fraud and identity theft, as well as with respect to an alleged failure to notify class members of the breach, even though the petitioner did not allege that he suffered those damages personally. In doing so, the **court referred to the Supreme Court's decision in Bank of Montreal v. Marcotte.⁸ Given the significant factual differences between Marcotte and Zuckerman, the clearly limited scope of the Supreme Court's reasons, and the potential impact of**

the Zuckerman decision on defendants' already limited rights at the authorization stage, the court's reference to Marcotte in this context may be questioned.

That said, the Zuckerman decision is noteworthy in that it illustrates the courts' apparent willingness to authorize privacy class actions that take into account potential fraud or identity theft, as well as any failure to notify affected customers.

Takeaways for Businesses

This case provides a number of takeaways for businesses on how to manage privacy breaches. It is interesting to note that the court authorized a common question on Target's alleged failure to notify affected customers . While breach notification is not yet mandatory in most Canadian provinces (it is only mandatory in Alberta), organizations may still decide to notify on a voluntary basis, especially if it is open to customers to argue that their damages were exacerbated because they did not receive timely notification.

Moreover, given that one of the common questions authorized against Target pertained to the cost of credit monitoring services, organizations which manage security incidents involving personal information may consider paying for such services (in cases that warrant them). This may be considered as a mitigating factor when assessing the damages sustained by customers.

The Zuckerman case may also serve as a warning of the extent of the potential consequences of a data breach, given the court's authorization of a common question pertaining to punitive damages. In response, businesses may wish to invest in prevention and ensure that they have adequate security measures in place, as well as an appropriate privacy governance framework. This will become even more important **when the new notification and recordkeeping requirements in the Personal Information Protection and Electronic Documents Act come into force. These requirements provide** that it will be a criminal offence for an organization to knowingly fail to report breaches, punishable by significant fines.

Finally, **the Zuckerman decision may also serve as a warning to businesses that their actions in one jurisdiction (in this case, the United States) can lead to significant legal exposure in another (i.e., Québec), in situations where their customer bases extend beyond provincial, state or national borders.**

¹ 2017 QCCS 110.

² Ibid. at para. 40.

³ 2008 SCC 27.

⁴ 2015 QCCA 1820.

⁵ 2012 QCCS 958.

⁶ 2015 QCCS 168.

⁷ Supra note 1 at para. 73.

⁸ 2014 SCC 55.

By

[Christopher C. Maughan](#)

Expertise

[Cybersecurity, Privacy & Data Protection, Class Actions](#)

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2024 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.