JUNE 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Settlement of Walmart Canada Photo Centre Data Breach Lawsuits – Lessons Learned

Canadian class action lawsuits over the Walmart Canada Photo Centre data breach were settled in May 2017. The lawsuits and settlement provide useful lessons for Canadian organizations that collect and process sensitive customer information.

The Data Breach

The Walmart Canada Photo Centre website, operated by Vancouver-based service provider PNI Digital Media ("PNI"), was the victim of a cyber-attack that installed malware on PNI's data centre servers to collect customers' credit card data and other personal information (e.g. names, emails and account passwords). After learning of the incident, Walmart Canada suspended the Photo Centre website, notified the Office of the Privacy Commissioner of Canada, engaged an independent consultant to conduct an investigation of the incident, and notified potentially affected customers.

Walmart Canada advised Photo Centre customers to closely monitor their credit card transactions and contact their financial institutions if they suspected irregular credit card activity, and recommended that customers change their passwords for other sites or services that were the same as their Photo Centre password. Walmart Canada did not offer a free credit monitoring service to all affected customers.

The Class Action Lawsuits

A representative plaintiff brought a national class action lawsuit in Ontario courts against Walmart Canada and PNI seeking $550 million in damages and other remedies (including a funded credit monitoring program) on behalf of Canadian customers who used the Walmart Canada Photo Centre website during the relevant period and whose personal information might have been compromised by the data security incident. A parallel class action lawsuit was commenced by another representative plaintiff in Saskatchewan courts.

The Statement of Claim in the Ontario action invoked various legal causes of action, including negligence, breach of contract and breach of duties imposed by common law and statute. The Statement of Claim included detailed allegations that Walmart Canada and PNI failed to adequately protect customer data, including:

- use of inadequate data encryption;
- engagement of personnel or contractors with inadequate skills, education, training and expertise;
- failure to use an outside, secure payment service;
- failure to use adequate technological security measures (e.g. firewalls, encryption, up-to-date hardware, software and security protocols, and protection against known vulnerabilities);
- failure to heed warnings about inadequate security and related risks;
- failure to follow industry standards and guidelines (e.g. PCI-DSS) for the protection of personal information and financial information; and
- failure to establish and effectively implement an internal computer security protocol.

The Statement of Claim also alleged that Walmart Canada and PNI breached duties and engaged in "reprehensible conduct" by failing to give affected customers timely notice of the breach and timely advice about mitigating credit card fraud risks.

The allegations in the Statement of Claim were not proven in court, and Walmart Canada and PNI denied any wrongdoing or liability of any kind.

The Settlement

The parties agreed to settle both class action lawsuits, subject to court approval. The Ontario court certified the class action for settlement purposes in December 2016. The Saskatchewan court conditionally approved the payment of legal fees to the Saskatchewan plaintiff in April 2017. The Ontario court approved the settlement in May 2017. The main terms of the settlement are as follows:

- **Credit Monitoring**: Walmart Canada and PNI will pay the costs of a one-year credit and identity theft monitoring service (or reimbursement of previously incurred costs for a similar service) for affected customers. The maximum cumulative total available for credit monitoring for all affected customers is $350,000.

- **Recovery of Expenses**: Walmart Canada and PNI will reimburse affected customers for their out-of-pocket losses, unreimbursed charges and time spent remedying issues traceable to the data security incident (at $15 per hour for up to five hours) to a maximum of $5,000 for any one customer. The maximum cumulative total available for recovery of expenses for all affected customers is $450,000.
- **Administration Costs**: Walmart Canada and PNI will pay up to $250,000 for the reasonable costs of administering the settlement, including the costs of a court-appointed independent claims administrator.
- **Plaintiffs' Legal Fees**: Walmart Canada and PNI will pay a total of $500,000 as legal fees (including disbursements and taxes) for the plaintiffs' lawyers for both class action lawsuits.

Lessons Learned

The Walmart Canada Photo Centre data breach lawsuits and settlement provide useful lessons for Canadian organizations that collect and process sensitive customer information.

- **Governance Framework**: An organization should establish a documented, comprehensive information security governance framework to ensure that appropriate practices, procedures, policies and systems for the protection of personal information and payment card information are established, consistently understood and effectively implemented. For more information, see BLG Bulletin *Regulatory Enforcement Action Emphasizes Need for Information Security Governance Framework*.
- **Supply Chain Cyber Risk Management**: An organization's cyber risk management program should include risks arising from suppliers of products and services used by the organization for its internal purposes or integrated into the organization's products or services, and from business partners with access to the organization's systems or who might otherwise be a risk to the organization's cybersecurity posture.
- **Data Breach Response**: An organization should have a comprehensive and suitable data security incident response plan and a trained incident response team. The plan should be consistent with applicable law, regulatory guidance and current best practices, and should be designed and implemented by a multidisciplinary team, including public relations advisors, senior management and legal counsel. For more information, see BLG Bulletin *Data Security Incident Response Plans – Some Practical Suggestions*.
- **Data Breach Notification**: An organization should give timely notice of a data security incident to affected individuals and organizations (including payment service providers), regulators and law enforcement in accordance with data incident notification obligations under statute, contract and generally applicable common law and civil law. For more information, see BLG Bulletin *Data Incident Notification Obligations*.
- **Litigation Risk Management**: An organization should carefully consider whether to voluntarily offer to provide affected customers with reasonable remedies (e.g. credit and identity theft monitoring and limited reimbursement for documented out-of-pocket costs) in order to reduce the incentives for class action plaintiffs to commence costly litigation. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com