

## ADVERTISING & MARKETING BULLETIN

October 2007

### **DATA/PRIVACY BREACHES ON THE RISE – IS YOUR BUSINESS PREPARED?**

The Federal and Alberta Privacy Commissioners issued a joint finding last month which concludes that the data/privacy breach that hit Winners and HomeSense earlier this year was both foreseeable and preventable. In addition, the finding notes that the companies did not comply with either the federal or Alberta private sector privacy laws.

Though many companies properly assess the need for disclosure and err on the side of their customers, there is currently no law in Canada which makes mandatory the disclosure of a privacy breach that compromises personal data, even if it involves sensitive information (save certain health-related data).

The House of Commons Standing Committee on Access to Information, Privacy and Ethics was troubled by this when they convened in late 2006 and early 2007 and drafted a set of recommendations to Parliament to help deal with this issue. These recommendations, including a requirement to notify the Office of the Privacy Commissioner of Canada in certain instances of a breach, were presented to Parliament in May 2007 and are purportedly still under review.

In the meantime, the Office of the Privacy Commissioner of Canada - still troubled by the lack of perceived accountability to the public with regard to such breaches - has issued their recommended “Key Steps For Organizations In Responding To Privacy Breaches.” The four- step approach with accompanying checklist was developed with the input and assistance of more than twenty stakeholders including corporations such as Bell Canada and IBM as well as watchdogs like the Consumers Council of Canada.

The first step is identified as “Breach Containment and Preliminary Assessment” and involves eliminating any threats and ascertaining the nature and scope of the intrusion or loss. It is suggested that one individual with sufficient authority lead the investigation and work quickly to complete this task. This step could involve law enforcement, if the breach is criminal in nature, or simply be an internal matter, if the breach is due to inadvertence.

Secondly, it is suggested that one “Evaluate the Risks Associated with the Breach” which involves looking at the myriad of factors at play including the sensitivity of the data in question; the usefulness of the compromised data to a would-be criminal; and the ease of access to the data if found, such as in the case of encrypted software. This is the step that helps one determine if a public disclosure is necessary under the circumstances, with focus on the foreseeable harm that could come from the breach.

The third step is “Notification” which should be done if it can help avoid or mitigate the harm to the affected individual. Notification should occur as soon as reasonably possible following the assessment of the breach unless there is a criminal investigation underway, in which case law enforcement should be consulted with respect to any such notification. The preferred method of notification is direct – by phone, letter, email or in person but, where such notification would be prohibitive due to cost or another factor, indirect notification, such as by way of the media, websites or posted notices can suffice. Intuitively, as the risk of harm to the affected person increases, so to does the onus to contact them directly. Notification does not only involve the public either – it is also suggested that the appropriate Provincial Privacy Commissioner be notified to assist in the matter as well as other appropriate regulatory bodies, insurers, credit and financial companies or any other organization related to the breach.

The fourth and final step, “Prevention of Further Breaches” takes place relatively later than the quick and turbulent first three steps and is a chance to review operating procedures, IT systems, employee training and security protocols to avoid a future reoccurrence. The level of effort put in at this stage should reflect the seriousness of the breach that has just been dealt with and its systemic or isolated nature with the ultimate goal of producing a longer-term plan of action.

Together, these steps assist any organization which holds private data to properly respond to that data being compromised. They also provide a road map for such organizations to best help those who have been affected by a breach to eliminate or mitigate its harmful effects. Without such an action plan, some companies may resort to doing nothing and hoping the problem goes away – which can lead to serious consequences for the affected people, such as identity theft, which could then lead to very significant repercussions for the organization - such as a huge loss of goodwill or a class action lawsuit.

The recent publication of these guidelines in Canada (and publication of similar guidelines in other jurisdictions such as New Zealand) reinforces the need for all businesses that handle personal information to have a security plan in place to protect that information and to respond in the event of a data/privacy breach. While these guidelines are not the law in Canada, one can be sure that it will not take too many more headlines involving millions of credit card numbers before Parliament makes these or similar recommendations the law – as is the case in many U.S. states.

For instance, Minnesota law enacted earlier this year prohibits any business that accepts credit, debit or stored value cards in Minnesota from retaining certain card data after a transaction has been authorized. The law also permits the financial institutions that issue these cards to recover the costs of a privacy/data breach from businesses that retain prohibited data in violation of the law. It is expected that many other states (including California, Illinois, Massachusetts, Connecticut and Texas) will follow.

Bottom line: prudence dictates that businesses begin implementing data/privacy breach response regimes so as to diminish the likelihood of a breach occurring or at least to be better prepared to deal with the fallout when such a breach does occur.

*Written by Bill Hearn and Andrew Warman.*

---

*The foregoing provides only an overview. Readers are cautioned against making any decisions based on this material alone. Rather, a qualified lawyer should be consulted.*

---

#### **ABOUT McMILLAN BINCH MENDELSON LLP**

McMillan Binch Mendelsohn LLP, one of Canada's leading business law firms, is committed to advancing our clients' interests through exemplary client service combined with thoughtful and pragmatic advice. The firm is a values-driven organization that takes a dynamic and sophisticated approach to providing practical and creative solutions to its clients. Its client first, team-based approach draws effectively upon our diverse expertise. The firm has a national, cross-border and international practice and has grown to be one of the top 20 largest firms in Canada. The firm is agile and flexible, committed to always striving for excellence. For additional information visit [www.mcmbm.com](http://www.mcmbm.com).

*For further information please contact your McMillan Binch Mendelsohn LLP lawyer or one of the Practice Leaders of our Advertising & Marketing Group listed below:*

#### **PRACTICE LEADERS**

Sharon Groom	416.865.7152	<a href="mailto:sharon.groom@mcmbm.com">sharon.groom@mcmbm.com</a>
Bill Hearn	416.865.7240	<a href="mailto:bill.hearn@mcmbm.com">bill.hearn@mcmbm.com</a>

## **McMILLAN BINCH MENDELSON**

TORONTO | TEL: 416.865.7000 | FAX: 416.865.7048

MONTRÉAL | TEL: 514.987.5000 | FAX: 514.987.1213

[www.mcmbm.com](http://www.mcmbm.com)

**2**