Data Breaches: Worth Noticing?

Executive Summary

This report was prepared by the Public Interest Advocacy Centre.

This report examines data breach notification in Canada in the private sector in general and in particular whether the proposed federal data breach notification law (Bill C-12) is adequate to protect Canadian consumers.

"Data breaches" are a loss, unauthorized access to or unauthorized disclosure of individuals' personal information by an organization holding that data. At present, only Alberta law requires reporting of private sector data breaches. Federally, such data breaches presently are covered by voluntary guidelines from the Privacy Commissioner of Canada.

The report concludes that the proposed data breach notification requirements in Bill C-12 grant excessive discretion to organizations that have had a data breach, allowing them unilaterally to characterize the breach as non-harmful to consumers. In so doing, organizations gain the benefit of a largely unreviewable decision in the face of a manifest and undeniable conflict of interest. The result is likely to be a vast underreporting of serious data breaches, which puts consumer welfare at excessive risk.

Therefore, PIAC supports an "Alberta model modified" data breach law at the federal level.

Recommendations include the following legislative changes (as amendments to Bill C-12 or additions or amendments to provincial legislation):

1. **There should be a duty to report all data breaches to the relevant privacy commissioner, either "as soon as reasonably possible" or within a short time window such as 48 hours;**
2. **There should be clear monetary penalties for not reporting to the privacy commissioner;**
3. **The privacy commissioner should decide on customer notification, based on a harm test. This test should be objective and based on the standard of "real risk of significant harm";**
4. **The privacy commissioner should be given the power to order an organization to report a breach to customers. Orders to notify customers should be made public as should the name the organization involved;**

5. **The privacy commissioner should have adequate audit powers to examine corporate data security practices and in particular to examine an organization's data breach notification preparedness and response;**
6. **The adequacy and effectiveness of the data breach regime should be separately evaluated at the time of the next review of PIPEDA or provincial privacy legislation.**

In addition, consideration should be given to the following recommendations independent of the legislative framework for breach notification:

7. **The privacy commissioner should create a dedicated data breach division, with adequate staffing, to address only data breaches.**
8. **The privacy commissioner should convene a "data breach advisory board" to bring current corporate information security expertise, consumer protection expertise and government regulatory expertise to bear on the question of data breaches.**
9. **The privacy commissioner should take a lead role in informing Canadians of how breach notification works, including a dedicated web page and online resources.**

Acknowledgment

PIAC received funding from Industry Canada's Contributions Program for Non-Profit Consumer and Voluntary Organizations to prepare the report. The views expressed in the report are not necessarily those of Industry Canada or the Government of Canada.

December 2011

Published January 2012