Submission to Industry Canada
Following the Stakeholder Consultation on the Proposed Model for Data Breach Notification

Public Interest Advocacy Centre
ONE Nicholas St, Suite 1204
Ottawa, Ontario
K1N 7B7
Tel: 613-562-4002 ext.25
Fax: 613-562-0007

April 25, 2008

OVERVIEW

The Public Interest Advocacy Centre (PIAC) appeared at the stakeholder consultation meeting held by Industry Canada on April 11, 2008 in Ottawa regarding a Proposed Model for Data Breach Notification. At the close of this meeting, it was indicated that parties could submit final comments on the proposed model. These are the comments of PIAC.

1. NO DEFINED CRITERIA, NO ENFORCEMENT

The discussion of data breach notification at this meeting is largely academic if companies and governments face no requirement to report to either the Office of the Privacy Commissioner of Canada (OPCC) or individuals and further if they face no sanction for not reporting a data breach incident that is required to be reported.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Report suggested a requirement to report to the OPCC for certain defined breaches of personal information and it recommended some form of enforcement mechanism. The Committee recommended in part:

> ***Recommendation 23***
> The Committee recommends that PIPEDA be amended to include a breach notification provision **requiring** organizations to report **certain defined breaches** of their personal information holdings to the Privacy Commissioner. [emphasis added]
>
> […]
>
> ***Recommendation 25***
> The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, **penalties for failure to notify**, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud. [emphasis added]

The present proposal fails in two respects. Firstly, it offers no requirement to report a breach when certain data elements are lost and secondly, it offers absolutely no enforcement mechanism whatever.

The present Industry Canada proposal either consciously or unwittingly has confused the ETHI Committee's wish for discretion in the Privacy Commissioner to order a breach notification to affected individuals (Recommendation 24), after being compulsorily notified by an organization of a defined data breach, with a discretion on the part of the affected organization to determine what constitutes a "material" breach. The present proposal then compounds the ineffectiveness of giving the organization the discretion to determine what

criteria should lead to reporting to the OPCC by avoiding any meaningful penalties for not reporting.

The only possible check on an organization's refusal to notify as per the guidelines would be the threat of an Office of the Privacy Commissioner of Canada (OPCC) audit – itself so rarely used as to be practically useless – or a possible complaint by an individual to the OPCC. Neither sanction is new and neither one outweighs the incentive to companies to under-report or not report data breaches due to the inherent conflict of interest they face in reporting themselves and the possibility of legal liability for a breach. At the very least an incident will likely have some detrimental, if transient, effect upon the public perception of organization. Since most companies are risk managed, they may well conclude under this proposal that the risk to reputation alone is higher than the risk of any sanctions, such as they are, for not reporting.

While it is true the Industry Canada Proposal indicates the Privacy Commissioner may report on material data breach notifications in her Annual Report to Parliament, there are no criteria on what she should report (number of complaints, type of breach, sector of the economy, etc.). Given the comments of the assembled banking, retail and other business interests at the April 11, 2008 consultation meeting, it is clear from their comments that they do not support such detailed reporting and indeed would actively resist any attempt to detail a particular data breach in the annual report. This "power of reporting" therefore also is likely a dead letter without sufficiently clear criteria, which the present proposal does not offer.

Recommendations:

PIAC continues to recommends that PIPEDA be amended to include a similar notification requirement to that contained in California's Bill 1386. Specifically, PIPEDA should impose a legal "duty to notify" upon any organization in Canada that suffers a loss or theft of specified personal information they hold about Canadians. Similar to the California legislation, and as recommended by the ETHI Committee, PIPEDA's notification provision should include the ability to impose fines or take other enforcement action for a failure to notify in accordance with the law.

NO STANDARD, NO CRITERIA

Even if Industry Canada persists in ignoring the two key elements of the ETHI report outlined above and instead adopts a more discretionary standard for both determining the seriousness of the breach and the need to notify, the present "test" for this as outlined in the consultation proposal is inadequate to result in notifications except in the clearest and most egregious cases, and perhaps not even then.

The slide presentation made at the consultation meeting of April 11, 2008 states the proposal "leverages existing guidelines produced by the federal and provincial privacy commissioners". In fact, it adopts the same guidelines approach of leaving significant discretion

in the organization, not the privacy commissioner, to determine whether a breach is important enough to warrant reporting and if it is also serious enough to notify customers.

The actual standard for this discretion, as stated in the proposal, has two serious flaws. First, the standard requires notification of affected individuals only when there is a "high risk of significant harm" to the individuals, as determined by the organization. As stated in our earlier comments, this standard leaves many potentially dangerous situations with no notification to customers or consumers at all. There may be situations in which involve a low risk of significant harm, or a high risk of moderate harm that remain unreported. Also, this determination is not made by a neutral third party but by the party suffering the breach itself. The organization, however, has an interest in not notifying customers following a breach – both from a cost and reputation perspective. The organization is not expert, likely, in the possible criminal uses of the information and may not have appreciated fully the manner or extent of the breach. Lastly, there is an assumption underlying this discretion being housed in the organization that there are proprietary rights held by the company to the personal information that trump the privacy rights accorded to Canadians by PIPEDA. Since nearly every data breach is likely a violation of PIPEDA, allowing such discretion to remain in the organization amounts to a "cover-up" of PIPEDA violations on the part of the organization – breaches that individuals could bring to the OPCC to investigate, if only they knew. Surely it is a poor policy choice to design a standard for breach reporting that actively undermines the fundamental purpose and spirit of the Act. Such a standard of discretion is no standard at all but rather *carte blanche*.

Second, the "criteria" for determining the reporting (to the OPCC) under the "material breach" threshold are not criteria but instead are factors. "Sensitivity of the information" is meaningless without a spelling out of the criteria, such as personal health information, financial information or sexual preference information. Likewise, a statement of "nature and number of data elements" should list them (and we understand that Industry Canada may be considering dropping these quite definable, yet key criteria, in response to comments from only industry representatives at the April 11, 2008 meeting). Unless the Industry Canada proposal recommends a listing of specific criteria in the regulations to supplement the stated "criteria" (really unquantified factors) in the proposal, this threshold likewise will become a meaningless "in the eye of the beholder" subjective standard.

Recommendations:

Objective, reasonable and measurable standards for breach notification have already been set by over thirty U.S. states. While there can be debate over these standards, leaving them vague and undefined, or to be determined by the subjective view of the organization that has the most to lose from reporting does a greater harm to the public than any possible harm in requiring breach notification to organizations under a clear set of rules. Canada should at the least be adopting the standards required by the California breach notification statute and indeed should be looking at them for deficiencies when they are compared to PIPEDA (such as requiring notification of lost IP addresses – which has been found to be "personal information" in Canada by the OPCC), not providing an amendment which amounts to little more than the arbitrary discretion to report which companies now enjoy.

NO TRANSPARENCY, NO REPORTING

There is an assumption on the part of Industry Canada that there will be a reporting of "material" breach notification information that is made available to the Privacy Commissioner "on an aggregate basis". This may not in fact occur or be as robust as necessary for the policy goals of understanding identity theft and encouraging companies to invest in data security.

Industry Canada's March 27, 2008 Proposed Model lists a number of reporting categories which will be required to be considered when deciding whether a breach is "material" and thus requires reporting to the OPCC, including "organization name and sector", "circumstance of the breach", "dates of incident and its discovery", "the number of individuals or records involved", "types of personal information involved", "what notification has been undertaken" and "steps to contain the breach". However, at the April 11, 2008 meeting, several participants, notably banks, insisted that any such "breach notification reports" would be classified as "investigation" documents and presumably thus made unobtainable under *Access to Information Act* requests. PIAC's concern is that such reports, and by implication any of their content, will be treated by the OPCC as confidential. As a result, there may be little for the OPCC to aggregate and the reports, such as they are, may be quite useless for research or for press reports. It also has been PIAC's direct experience that the OPCC refuses to "name names" under PIPEDA, and that companies breaching individual privacy are only identified if the complainant makes public their own copy of the Commissioner's finding. Finally, the Annual report will only appear some time (up to 18 months) after the data breach reported to the OPCC. The public deserves to know some details of "material" breaches in a timely manner.

Recommendations:

If indeed any of the policy goals of transparency, understanding and deterrence are to be effected by reporting, the OPCC should be directed to file information akin to that required for the material breach report, removing only those details that truly represent a threat to the security of the organization, truly threaten a competitive advantage or trade secret, or otherwise outweigh the public interest in the transparency policy goals. This unredacted information should, at the very least, be published by the OPCC with her Annual Report to Parliament, but preferably as soon as possible.

Finally, PIAC reiterates its and CIPPIC's call for an on-going public Internet-based directory of data breaches, maintained by the OPCC and updated regularly, rather than a once a year report, so that Canadians, the press and researchers can identify risk to themselves and study trends and possibly identify new directions in avoiding data breaches and the social cost they inflict on individuals. Such transparency would also be the only means available to the public to gauge if the standard of "material" breach reporting to the OPCC, and notification only when there is a "high risk of significant harm" are sufficient to protect them from identity theft and privacy violations when, quite out of their control, organizations suffer a data breach.

*** End of Document ***