ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-007

IPSOS NORTH AMERICA

November 10, 2010

(Case File #P1704)

I. Introduction

[1] On October 26, 2010, I received a report from Ipsos North America (Ipsos) of an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information of individuals in Alberta. Based on the information reported to me, I have decided that there is a real risk of significant harm to those individuals as a result of the incident, and therefore I require that Ipsos notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under section 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of signification harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] Ipsos is a global survey-based market research company, with an office in Alberta. Ipsos qualifies as an "organization" pursuant to section 1(1)(i) of PIPA.

[6] The personal information at issue is that of Ipsos employees who are resident in Alberta, and includes employee names, Social Insurance Numbers (SINs), dates of birth, home addresses and contact phone numbers. This is information about identifiable individuals and qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[7] In considering whether to require Ipsos to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[8] On October 26, 2010, I received a written report from Ipsos describing an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information of individuals in Alberta

[9] My Office corresponded with Ipsos by telephone and email between October 28-30 to obtain additional information regarding this incident.

[10] Ipsos reported that on October 7, 2010, an Ipsos employee's laptop containing personal information of Ipsos employees was lost in the course of travel. The laptop was left in an overseas airport, and to date has not been recovered.

[11] The personal information at issue was in an Excel file stored on the laptop, and includes employee names, SINs, dates of birth, home addresses and contact phone numbers.

[12] Ipsos reported that "the device had both a bootable password and windows password" but personal information stored on the laptop was not encrypted.

[13] Ipsos reported that of the individuals that could have been affected by this incident, 27 are residents of Alberta. Ipsos advised that it would be notifying all affected individuals, and provided a draft copy of the notification that would be sent.

[14] Ipsos reported that it "has implemented additional quality controls regarding laptop management to avoid similar incidents in the future."

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[15] Pursuant to section 37.1 of PIPA, I have the power to require Ipsos to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require Ipsos to notify individuals in this case, I must consider whether there exists a "real risk of significant harm" to those individuals as a result of the incident.

[16] In order for me to require that Ipsos notify individuals, there must be some harm – some damage or detriment or injury – that could be caused as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[17] In this case, the personal information at issue is of high sensitivity as it includes employee names, SINs, dates of birth, home addresses and contact phone numbers.

[18] This is information that could be used to cause significant harm to individuals, and provides comprehensive individual profiles that could be used to commit identity theft and/or fraud.

[19] In order for me to require Ipsos to notify individuals, however, there must also be a "real risk" of harm to individuals as a result of this incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[20] In deciding whether there exists a "real risk" of harm in this case, I noted that the laptop in this case was lost and not stolen, and that Ipsos reported that "[a]t this time, Ipsos is not aware of any improper use of the personal information contained in the files."

[21] Despite these considerations, I have nonetheless decided there is a real risk of significant harm to individuals in this case. Ipsos confirmed that the laptop was protected by a bootable password and windows password, which could be relatively easily bypassed. Once bypassed, the personal information of Ipsos employees would be readily accessible.

[22] I also considered that to date, and despite Ipsos' efforts, the laptop has not been recovered. In my view, if the laptop was found by an individual having no nefarious intentions, it would likely have been turned in to airport authorities. The fact that it has not been turned in suggests a real possibility that anyone who may have found it has decided to keep it, either for personal use or to sell for profit. If the finder is of this mindset, and considering that personal information stored on the laptop could be readily accessed if the password protections were bypassed, I believe there is a real risk of significant harm to individuals in this case.

V. Decision

[23] Based on the information reported to me by Ipsos, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require Ipsos to notify individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, and confirm in writing to my Office that it has done so on or before December 1, 2010 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner