ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-028

Britec Computer Systems Limited

September 13, 2011

(Case File #P1949)

I. Introduction

[1] On August 2, 2011, I received a report from Britec Computer Systems Limited (Britec) of an incident involving the loss of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Britec notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under s. 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 significant 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] I have jurisdiction in this matter because Britec is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

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

III. Background

[7] On August 2, 2011, I received a written report from Britec describing an incident involving the loss of personal information.

[8] On August 25, 2011, my Office contacted Britec to request that it provide additional information concerning the incident, in order for me to determine whether to require Britec to notify individuals under subsection 37.1(1) of PIPA.

[9] My Office received Britec's response on August 25, 2011. One subsequent phone call for follow up information occurred between Britec staff and my office on August 29, 2011.

[10] The circumstances of the incident as reported to me by Britec are as follows:

- Britec's Calgary office was broken into on July 27, 2011.
- 1 unencrypted external hard drive, 1 unencrypted flash drive and 3 password protected lap tops were stolen.
- The incident was discovered when staff came to work the morning of July 27, 2011.
- The stolen mobile devices contained human resources information for between 60 to 100 current and former staff.
- The breach affected current and former employees in Ontario, British Columbia and Alberta.
- Information contained on these devices included but is not limited to;

    - Full name;
    - Contact information including home addresses;
    - Social Insurance numbers;
    - Payroll information including bank account numbers;
    - Offer letters containing salary and benefit information;
    - Reprimands received by some employees; and
    - Other human resource information may have also been included that related to individual employees' job performances.
- Police were notified of the theft on July 27, 2011.
- Britec notified the BC and Alberta Privacy Commissioners of the loss on August 2, 2011.
- Britec notified all current staff of the data loss verbally July 27, 2011 and in writing on the same day. Former employees were notified via letters that were mailed out on August 2, 2011.
- Britec has begun implementing a more secure system for the management of all human resource and financial data in response to this loss.

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

[11] Pursuant to section 37.1 of PIPA, I have the power to require Britec 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 Britec to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

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

[13] In this case, the personal information at issue is of moderate to high sensitivity as it includes full names, addresses, banking information and social insurance numbers.

[14] Britec also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm. I further note that for those employees whose disciplinary records were lost, the disclosure of that personal information could lead to hurt, humiliation and reputational damage which is also, in my view, a significant harm.

[15] In order for me to require Britec to notify its past and present employees however, there must also be a "real risk" of significant harm to the employees as a result of the incident. This standard does not require that significant 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.

[16] In deciding whether there exists a "real risk" of harm in this case, I considered the following information; the office was broken into and this clearly indicates malicious intent. The Social Insurance numbers, banking information and home addresses all pose a risk of identity theft while the loss of performance information such as reprimands pose a risk of humiliation for the affected individuals. Due to these facts, and that the information has not been recovered to date, there is a real risk that the information may be used to cause significant harm.

[17] Given the information reported by Britec, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the personal information at issue is of moderate to high sensitivity and includes banking information, social insurance numbers, and disciplinary records of individuals. This is information that could be used to commit identity theft or harm reputations.

V. Decision

[18] Based on the information reported to me by Britec, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Britec to notify affected individuals. I understand Britec has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on August 2, 2011; therefore I will not require Britec to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner