ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-13

GALLIVAN AND ASSOCIATES STUDENT NETWORKS INC.

April 25, 2012

(Case File #P2074)

I. Introduction

[1] On March 1, 2012, I received a report from Gallivan and Associates Student Networks Inc. ("Gallivan" or the "Organization") 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 Gallivan notify 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 Gallivan 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 Gallivan 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 March 1, 2012, I received a written report from Gallivan describing an incident involving the loss of personal information that was contained in a spreadsheet stored on a portable memory device.

[8] Gallivan manages the Health and Dental Plan ("the Plan") for students at Bow Valley College ("BVC"). BVC collects the personal information at the time of registration of students, and subsequently discloses, with consent of the student, it to Gallivan for the purposes of administering the Plan. Gallivan establishes coverage for the students and enrolls them in the Plan. Gallivan is responsible for removing students once they no longer have coverage. In my view, Gallivan has control of the information at issue in this incident, and is responsible under section 34.1 of PIPA to notify me of any loss of 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.

[9] On March 5, 2012, my Office contacted Gallivan to request that it provide additional information concerning the incident, in order for me to determine whether to require Gallivan to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mails between March 5 and April 17, 2012.

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

- A Gallivan staff member went to use a portable memory device (flash drive) and could not locate it. After an extensive search, she reported it missing. It is unknown if it was stolen or lost inadvertently.

- The device contained a spreadsheet, and the personal information at issue in this case that was on the spreadsheet includes the following:
    - Student Name;
    - Date of birth;
    - Gender;
    - Student ID number;
    - Program of study;
    - Grant funded or exempt.

- The flash drive was not encrypted or password protected.
- The data on the device could be easily accessed using standard software, and while some of the information (coding) would not make sense or be usable, the name, date of birth, and gender and student ID number are identified as such.
- The number of affected individuals in this case is 2557.
- Following the incident, Gallivan reported it commenced an audit of their service protocols, including dealing with individuals, their information, and the handling of information in all situations.

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

[11] As noted above, pursuant to section 37.1 of PIPA, I have the power to require Gallivan 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 Gallivan 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 interpreting this phrase, it is clear that in order for me to require that an organization notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to individuals 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] Gallivan noted that it was unlikely that the personal information contained on the flash drive could be used by itself to harm individuals (e.g. to access financial information, or to commit identity theft). Gallivan assessed the possibility of identity theft as low in this case.

[14] In my view, the personal information at issue in this case is of moderate sensitivity and could be used to cause significant harm to individuals. While name and date of birth alone may not necessarily be sensitive, when combined with other personal information elements, this is information that could reasonably be used to cause significant harm to individuals in the form of identity fraud or other financial fraud. The Canadian Anti-Fraud Centre has confirmed that an individual's name and birthdate can be used to commit identity theft.

[15] In order for me to require Gallivan to notify the affected individuals, however, there must also be a "real risk" of significant harm to the individuals 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 significant harm in this case, I considered the large number of affected individuals, and that the personal information on the flash drive was not encrypted and has not been recovered. All of the information on the flash drive could be accessed, read, saved, copied, e-mailed, etc. with minimal effort given that there was no encryption.

[17] Given the information reported by Gallivan, 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 type of information involved could be used to commit identity theft, which is a significant harm; a large number of individuals are affected; and the flash drive was not encrypted and has not been recovered.

V. Decision

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

Jill Clayton
Information and Privacy Commissioner