ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-005

FULL BARS COMMUNICATIONS INC.

October 7, 2010

(Case File #P1669)

I. Introduction

[1] On September 2, 2010, I received a report from Full Bars Communications Inc. (Full Bars) of an incident involving the loss of and unauthorized access to personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to some individuals as a result of the incident, and therefore I require that Full Bars notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] PIPA applies to to provincially-regulated private sector organizations in Alberta. I have jurisdiction in this case because Full Bars is an "organization", as defined in section 1(i) of the Act, operating in the province of Alberta.

[3] 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.

[4] 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.

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

III. Background

[6] On September 2, 2010, I received a written report from Full Bars describing an incident involving the loss of and unauthorized access to personal information.

[7] On September 21, 2010, my Office contacted Full Bars to request that it provide additional information concerning the incident, in order for me to determine whether to require that it notify individuals under subsection 37.1(1) of PIPA. My Office received Full Bars' response on September 21, 2010.

[8] The circumstances of the incident reported to me are as follows:

- On August 6, 2010, the owner of Full Bars discovered that his home garage had been burglarized and several items stolen, including two external hard drives containing the personal information of current and former employees and customers of Full Bars. He notified the Edmonton City Police of the incident.
- The external hard drives contained personal information current to approximately one week prior to the incident. The information on the two external hard drives was essentially identical but one was slightly more current than the other.
- The personal information of the current and former employees on the external hard drives consisted of names, addresses, phone numbers, Social Insurance Numbers, and driver's license numbers. The personal information of individual customers consisted of names and business phone numbers (not home phone numbers), truncated credit card numbers and in some cases, business addresses (not home addresses). The external hard drives were not encrypted.
- Full Bars verbally notified its current employees of the incident.

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

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

[10] In order for me to require that Full Bars 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.

[11] Although credit card numbers are highly sensitive, as the credit card numbers were truncated, I do not find that there is a real risk of significant harm to the customers whose credit card numbers were involved in this incident. It is unlikely that truncated credit card numbers, even with customer names, could be used for fraudulent purposes or to

perpetrate identity theft. Therefore, in my view, there is no real risk of significant harm and I will not require Full Bars to notify these individuals.

[12] In the case of the employees, however, the personal information at issue is of moderate to high sensitivity as it includes names, addresses, Social Insurance Numbers and driver's license numbers of the current and former employees.

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

[14] In order for me to require Full Bars to notify individuals, however, there must also be a "real risk" of harm to individuals as a result of the 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.

[15] I note that while Full Bars acted quickly to inform the police of this incident, the external hard drives were stolen, were unencrypted and have not been recovered.

[16] Given the sensitivity of the personal information of the employees at issue, and the fact the information was stolen and was unencrypted, I believe there is a real risk of significant harm to the current and former employees of Full Bars in this case.

V. Decision

[17] Based on the information reported to me by Full Bars, I have concluded there is a real risk of significant harm to the former and current employees as a result of this incident and I require the Full Bars to notify these individuals in accordance with the Regulations and confirm in writing to my Office that it has done so on or before October 28, 2010 or such other date as I may specify.

[18] I understand Full Bars has already notified its current employees of this incident but not its former employees.

Frank Work, Q.C.
Information and Privacy Commissioner