ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-003

CEDA INTERNATIONAL CORPORATION

January 6, 2011

(Case File #P1677)

I. Introduction

[1] On September 27, 2010, I received a report from CEDA International Corporation (CEDA) of an incident involving the unauthorized disclosure 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 CEDA notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] PIPA applies to provincially-regulated private sector organizations in Alberta. I have jurisdiction in this case because CEDA is an "organization", as defined in section 1(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 CEDA 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 27, 2010, I received a written report from CEDA describing an incident involving the unauthorized disclosure of personal information.

[7] On October 14, 2010 and November 9, 10, and 30, 2010 my Office contacted CEDA 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 CEDA's final response on December 14, 2010.

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

- On June 2, 2010, a CEDA employee in the Human Resources ("HR") department became aware that an HR folder containing the personal information dating back to 1999 of 104 employees of CEDA Environmental Fluid Solutions LP ("EFS"), a subsidiary entity of CEDA, was located on the CEDA employee public computer drive which was accessible to all CEDA EFS employees. The existence and location of the folder was reported to HR by an employee who had found the folder and reviewed his own file.
- The folder was located on the local screen within the EFS folder along with other folders accessible to the employees and titled "HR".
- CEDA estimated the HR folder had been created sometime between the end of January 2010 and March 22, 2010.
- CEDA conducted an audit of the material in question to determine what personal information was located in the HR folder. The personal information contained within the HR folder included the following:
    - Position/title information, resumes and offer letters;
    - Dates of birth, marital status, social insurance numbers, drivers license numbers and home contact information;
    - Rates of pay, banking information (including transit and account numbers), employee expenses, per diem information and Visa limits;
    - Discipline records, medical information, overtime information; and
    - Other HR information including suspensions, terminations and safety violations.
- As CEDA currently does not have software capable of auditing user access and activities, it was unable to determine whether any of the personal information had been accessed without permission. However, based on the information provided by the IT department, CEDA estimates that approximately 55 people would have had access to the information within the HR folder.
- On June 3, 2010 CEDA took immediate steps to secure the HR folder and restrict access to the appropriate HR personnel and necessary intellectual

property administrators. CEDA also developed and implemented a privacy policy which each CEDA employee is required to review and sign.

- In CEDA's opinion, the type of harm 104 EFS employees may be subject to if this information had been improperly accessed included possible credit fraud, financial loss, humiliation, loss of reputation and identity theft.
- CEDA is engaging various vendors to establish some options around monitoring, auditing and intrusion software which could be incorporated within its current organization. This suite of software tools will allow CEDA to maintain compliance with industry standards and ensure it operates securely and is protected from potential breaches and violations. It will also allow CEDA the ability to log and track user activities in the event of a compromise and allow database administrators to deliver accurate and timely reports on user activities.
- As CEDA was unable to positively determine the scope of unauthorized access, it has not yet notified any of the employees whose information was found in the HR folder and requests direction from the Office of the Information and Privacy Commissioner in this regard.

[9] The posting of the HR folder on an unsecured, internal public drive where it could be accessed by any employee constitutes, in my view, an unauthorized disclosure of the information.

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

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

[11] In order for me to require that CEDA 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.

[12] In my view, the personal information of the employees contained in the HR folder on the public drive is of high sensitivity as it includes names, addresses, dates of birth, Social Insurance Numbers, driver's license numbers and banking information as well as sensitive employee information such as rates of pay, discipline records, medical information, suspensions, terminations and safety violations.

[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. In addition, depending on the information contained in the folder, there may be

significant harm to the reputations of employees whose terminations, disciplinary records and/or medical information are contained in the folder.

[14] In order for me to require CEDA 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] CEDA did not provide an opinion as to the likelihood the HR folder had been accessed by someone without permission or, if it had been accessed, the likelihood that access of this information by an unauthorized individual would result in significant harm to an EFS current or former employee.

[16] I note that while CEDA acted quickly to secure the HR folder once its location had been discovered, the HR folder had been located on an unsecured public drive for an estimated period of three to five months and CEDA had no way to determine whether anyone who was not authorized to see the information had accessed the HR folder and viewed the sensitive personal information.

[17] Given the length of time the folder was on the public drive and the fact it was not buried beneath or within other folders a user would have to click through but readily and easily available for anyone to view, I am of the view that there is a real risk the HR folder was accessed by one or more individuals who were not authorized to view it.

[18] Given the sensitivity of the personal information of the employees at issue, and the fact the information was located on an unsecured public drive for an estimated period of three to five months during which it is likely individuals who were not authorized to access the folder, accessed and viewed the information, I believe there is a real risk of significant harm to the CEDA EFS employees whose information was contained in the HR folder in this case.

V. Decision

[19] Based on the information reported to me by CEDA, I have concluded there is a real risk of significant harm to the CEDA EFS employees (current and former) whose information was located in the HR folder as a result of this incident and I require the CEDA to notify these individuals in accordance with the Regulations and confirm in writing to my Office that it has done so on or before February 8, 2011 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner