ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-016

CEDA INTERNATIONAL CORPORATION

June 3, 2011

(Case File #P1870)

I. Introduction

[1] On May 10, 2011, I received a report from CEDA International Corporation ("CEDA") of an incident involving 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 individuals as a result of the incident, and therefore I require that CEDA 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 CEDA 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 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

[7] On May 10, 2011, I received a written report from CEDA describing an incident involving the unauthorized access to personal information.

[8] On May 19, 2011, my Office contacted legal counsel for CEDA to request that it provide additional information concerning the incident, in order for me to determine whether to require CEDA to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and email correspondence between May 19, 2011 and May 31, 2011.

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

- On April 6, 2011, an employee of one of the Edmonton offices of CEDA was searching in the "L" drive, an internal public drive on CEDA's computer system, for information concerning his eligibility for a service award. He opened a subfolder on this drive.
- The subfolder, which was displayed under another employee's name, contained a spreadsheet containing the names, social insurance numbers and bi-monthly salaries of 240 existing and former CEDA employees.
- The employee reported the incident to his supervisor. The information was removed from the system April 6, 2011.
- The employee whose name appears on the subfolder has no recollection of creating the spreadsheet and does not recall accessing or saving any information to the spreadsheet.
- The spreadsheet was created January 5, 2010, last modified January 21, 2010, and removed April 6, 2011. It was on CEDA's internal public drive for 15 months.
- Approximately 240 employees at this Edmonton location out of a total of 750-800 CEDA account holders were connected to the "L" public drive during the time the subfolder was accessible. Any other CEDA account user would have had to manually connect to the "L" drive if they were not located in the office where the incident occurred and CEDA informed my Office this would have been difficult.

- CEDA asserts that due to the fact that this was a subfolder with the name of a particular employee on it that the probability it was accessed by others during this time period is low. However, CEDA is unable to provide an audit trail as to whether or not the spreadsheet was accessed prior to this incident.
- CEDA recognized that access to social insurance numbers is highly sensitive personal information the disclosure of which presents a risk of identity theft, fraud and financial loss. However, CEDA emphasized in its submission that the drive was only accessible to employees within the Edmonton location.
- CEDA has shut down access to public folders in the "L" drive to prevent any further breaches. Employees requiring access to the "L" drive must go through an authorization process before information is released.
- CEDA stated in its submission that it is mindful of decision P2011-ND-003 issued by my Office on January 6, 2011, regarding sensitive personal information found on a CEDA public drive. CEDA asserts it is working to ensure CEDA's information technology systems contain proper security controls to prevent unauthorized disclosures of personal information and hopes to implement new controls, programs and processes by July 2011 with further document management solutions proposed for 2012.
- CEDA has also advised that it is currently performing a review of the entire internal system and will continue this review until the new software security system is in place.

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 those 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 this case, the personal information at issue is of high sensitivity as it includes name, social insurance number, and salary information for 240 current and former employees of one Edmonton location office of CEDA.

[13] CEDA 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.

[14] In order for me to require CEDA to notify the affected individuals, however, there must also be a "real risk" of harm to the employee 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] In deciding whether there exists a "real risk" of significant harm in this case, I considered that CEDA is unable to confirm by way of an audit trail whether or not the spreadsheet was accessed by any other employees. While the subfolder may be under the name of a specific employee, it did not prevent the employee who discovered it from opening up the subfolder and viewing its contents. The spreadsheet was accessible to approximately 240 employees for over a year. Even though the possibility of unauthorized access or disclosure occurred within an internal group of employees there is no way to confirm that no one else other than the employee who reported this incident accessed the information. The sensitivity of the information was also a factor in my determination of real risk of significant harm.

V. Decision

[16] Based on the information reported to me by CEDA, I have concluded that there is a real risk of significant harm to the affected individuals as a result of this incident.

[17] I require CEDA to notify individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation,* if CEDA has not already done so, and confirm in writing to my Office that it has done so on or before June 30, 2011, or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner