ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-07

CEDA INTERNATIONAL CORPORATION

June 25, 2012

(Case File #P2038)

I. Introduction

[1] 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.

[2] On December 5, 2011, CEDA International Corporation (the "Organization") provided notice of an incident involving the loss of or unauthorized access to or disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[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] The Organization is registered in Alberta as a Corporation. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information of approximately 50 of its employees:

- birthdates,
- drivers' licence numbers,
- qualifications,
- exit interviews,
- letters of reprimand and discipline,
- performance assessments,
- terminated employees' list and termination letters,
- incident reports,
- drug testing results,
- letters regarding alleged substance abuse, and
- a spreadsheet detailing workplace incidents and employees involved in the incidents.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On December 7, 2011, my Office requested the Organization provide additional information. The additional information was provided by the Organization between December 7, 2011, and March 15, 2012.

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

- Following a breach of personal information involving unauthorized access to personal information located on its internal "L" drive, which was reported to my

Office on May 10, 2011[1], the Organization undertook a review of the contents of its "L" drive.

- During this review, the Organization found documents containing the personal information at issue.
- The "L" drive is accessible by approximately 240 employees of the Organization.
- Access to the "L" drive was shut down on April 6, 2011, and all the personal information immediately removed.
- The length of time the personal information was accessible is unknown and varies depending on when the documents containing the personal information were created.
- There is no audit functionality on the "L" drive. As a result, it is unknown who accessed the personal information.
- As part of its systems review and the investigation into the breach, the Organization has implemented the following measures:
    - Plans to transition to a new system with audit capability are underway.
    - A document management system and records management structure is being developed.
- The Organization has not notified the affected individuals.

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

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

[11] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[12] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization indicated that the personal information at issue is highly sensitive and presents risks of hurt, humiliation and damage to reputation.

[14] I agree with the Organization that the personal information at issue in this incident is highly sensitive. The types of harm that could result from unauthorized access to the

[1] See Breach Notification Decision P2011-ND-003.

personal information in this instance are identity theft and fraud, harm to reputation, and humiliation. In my view, these are significant harms.

[15] In order for me to require the Organization to notify the affected individuals, there must also be a "real risk" of significant harm to the affected 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. There must be a cause and effect relationship between the incident and the possible harm.

[16] The Organization reported the incident does not pose a real risk of significant harm to the affected individuals for the following reasons:

- The "L" drive was an internal drive not accessible to the general public.
- The personal information was contained in embedded folders on the "L" drive. Therefore, the probability that any of 240 employees accessed the personal information is less than 10%.
- The personal information was discovered during a systematic review, not by an employee by accident.
- The personal information was immediately removed from the system when located during the Organization's review.
- Access to the system was shut down after April 6, 2011.

[17] In deciding whether there exists a "real risk" of significant harm in this case to the affected individuals, I considered the following factors:

- The personal information is highly sensitive.
- The length of time the personal information was accessible is indeterminate.
- The Organization cannot confirm that the personal information was not accessed by one or more of the 240 employees.

[18] In Breach Notification Decision 2011-ND-003, Commissioner Work decided that, despite the Organization's inability to confirm whether personal information in a folder that contained human resource information found on the "L" drive was actually accessed, there was a possibility that sensitive personal information was viewed or copied. Given the sensitive data elements and the length of time the information was potentially exposed, Commissioner Work decided there was a real risk of significant harm to the affected individuals and required the Organization to notify those individuals under section 37.1 of PIPA.

[19] Based on the information reported to me by the Organization and for the foregoing reasons, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident.

V. Decision

[20] I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation") and confirm in writing to my Office that it has done so on or before July 13, 2012.

Jill Clayton
Information and Privacy Commissioner