Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Pyramid Corporation (Organization)
Decision number (file number)	P2013-ND-45 (File #P2523)
Date notice received by OIPC	November 22, 2013
Date Organization last provided information	December 11, 2013
Date of decision	January 23, 2014
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information for 200 current and former employees of the Organization: • name, • trade (e.g. journeyman, electrician), • social insurance number, • hourly rate of pay. The incident also involved the following information for one employee of the Organization: • personnel file (name, address, date of birth, bank account number, employee acceptance letter, tax documents and resume).

	This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On November 22, 2013, the Organization's human resources officer reported to the Manager of Fleet/Security that an employee, prior to her termination, had forwarded 60 emails (unopened) from her business email account to her personal email account. In addition, personnel files of the terminated employee and her daughter (also an employee of the Organization) were missing. The terminated employee, who worked in the Organization's payroll department, had authorized access. • System audit logs confirmed that the employee had forwarded the business emails to her personal email account. • Of the 60 emails, two included personal information of approximately 200 current and former employees of the Organization, in spreadsheet form. • The Manager of Fleet/Security interviewed the terminated employee who stated: o she forwarded the emails to her personal "Hotmail" account so she would have all her personal emails, o she deleted the business emails from her personal email account without opening them, including the two that contained personal information of the Organization's current and former employees, o she took the two personnel files because she wanted to make copies of her and her daughter's resumes. She intended to return them the next day, o upon being contacted by the Manager of Fleet/Security, she returned the two personnel files with all documents intact, o she realized what she had done could be viewed as unethical. • The Manager of Fleet/Security reviewed the terminated employee's personal Hotmail account and confirmed that: o all "inbox" emails were non-work related. o the "deleted" box was empty. o there was nothing in the "sent" box to indicate the personal information of the current and former employees had been distributed any further.

	• The Organization did not review the employee's Hotmail account audit trail and cannot confirm that the employee did not access or save the personal information contained in the emails.
Affected individuals	201 affected individuals located in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the RCMP in Leduc, Alberta. • Cancelled the employee's password and username for her business email account. • Developing screening methods for prospective employees and user policies.
Steps taken to notify individuals of the incident	None
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization submitted that the harms that could result from this incident are fraud and identity theft. In my view, the information of the current and former employees is highly sensitive. It contains names, social insurance numbers and pay rates. I agree with the Organization that the types of harm that could result from unauthorized access to this information are identity theft and fraud. In my view, these are significant harms. I find that information contained in the personnel file that was taken from the Organization's premises – including name, date of birth, bank account number, and tax documents – is also highly sensitive. This information could be used to cause significant harm in the form of identity theft and fraud.
Real Risk The likelihood that the significant harm 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.	The Organization reported that it is uncertain of the sensitivity of the personal information involved; therefore, it considered there was no real risk of significant harm to the affected individuals. In my view, the likelihood of harm to the 200 current and former employees is increased because the personal information was sent outside the Organization without authority. Additionally, even though the Organization reviewed the employee's personal Hotmail account, it is unable to confirm that the employee did not open or save the two emails or the personal information they contained.

	I also find there is a real risk of harm to the individual whose personnel file was taken from the Organization in order to photocopy her resume. Although this individual is the daughter of the employee who took the file, there is no evidence before me to suggest the daughter authorized the photocopying or was aware the file was taken. Further, the file was removed from the Organization's premises without authority, and was not returned until the employee was contacted by the Manager of Fleet/Security, despite the employee's stated intention to return it the next day.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and the circumstances of this incident, I have decided that there is a real risk of significant harm to the affected individuals in this case. The personal information at issue includes sensitive identity information, such as names and social insurance numbers, in addition to pay rates. The information was removed from the Organization's premises without authority. The Organization has not confirmed that the employee did not access/save personal information in the emails. These factors contributed significantly to my decision.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and notify me in writing it has done so on or before February 7, 2014.

Jill Clayton
Information and Privacy Commissioner