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	Clarcor Inc. (Organization)
Decision number (file number)	P2015-ND-31 (File #P2919)
Date notice received by OIPC	November 20, 2014
Date Organization last provided information	January 14, 2015
Date of decision	May 15, 2015
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 the United States. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • job title, • date of birth, • gender, • address, • telephone number, • job code, • salary, • email address, • supervisor's name, • hire date, • employee number, and • Social Insurance Numbers (SINs) for four employees (two

	of which were Alberta residents). 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	• An employee of the Organization distributed employee benefit information by email to 12 employees in Canada. However, the information of all 12 employees was inadvertently sent to each employee (as opposed to each employee receiving only his or her own information). • The information was contained in an Excel spreadsheet in a "separate tab" that was not immediately visible to an employee unless he or she clicked on the tab. • The information was exposed for 3 weeks before the incident was discovered during an audit.
Affected individuals	A total of 12 employees were affected, including 3 Alberta residents.
Steps taken to reduce risk of harm to individuals	• The information was recovered and wiped from all computer servers, back-up systems and employee email accounts. • The Organization received signed confirmations from all employees stating that they no longer possessed the information. • Employees were reminded of their confidentiality oaths. • The electronic files were sent without passwords or encryption. The Organization has now implemented a policy prohibiting this practice.
Steps taken to notify individuals of the incident	Affected individuals were notified in a letter sent via email.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-	The Organization recognized the affected individuals may be at risk for fraud, identity theft and negative effects on credit reports. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud, as well as possible embarrassment/humiliation

trivial consequences or effects.	due to the relationships between co-workers. In my view, these are significant harms.
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, notwithstanding the sensitivity of the information, it believed that there was no real risk of significant harm to the affected individuals for the following reasons: • The information was only sent to internal employees, bound by a confidentiality clause. • The information was recovered and destroyed upon discovery of the breach. • All employees confirmed in writing that they no longer possessed the information. • The Organization reminded employees of their confidentiality oaths. • Due to the location of the data (a separate tab on a spreadsheet), it is not likely that the employees viewed the personal information. • During the three weeks that the information was exposed, the Organization received no indication from any of the affected employees that he or she had received the information. I agree these factors reduce the likelihood of harm resulting from this incident. However, while the Organization confirmed the personal information was no longer in the possession of the unauthorized recipients, it did not confirm that the information was not viewed by them. In the absence of such an assurance and given the length of time the information was exposed (3 weeks), I find that there remains a real risk of significant harm resulting from this incident.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The types of harm that could result from this incident are identity theft and fraud, as well as possible embarrassment/humiliation due to the relationships between co-workers. In my view, these are significant harms. The Organization identified a number of factors that reduce the risk of harm resulting from this incident; however, while the Organization confirmed the personal information was no longer in the possession of the unauthorized recipients, it did not confirm that the information was not viewed by them. In the absence of such an assurance and given the length of time the information was exposed (3 weeks), I find that there remains a real risk of significant harm resulting from this incident.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization notified the affected individuals in a letter dated November 4, 2014. Therefore, the Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner