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	Dufferin Construction Company, a division of CRH Canada Group Inc. (Organization)
Decision number (file number)	P2019-ND-038 (File #010963)
Date notice received by OIPC	November 30, 2018
Date Organization last provided information	November 30, 2018
Date of decision	February 27, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	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 information contained in job offer letters for 44 active and inactive employees, including: • name, • mailing address, • hire date, • job title, • wage/salary, and • vacation and benefits entitlement. In addition, for 24 of the employees, the information included: • benefits enrollment information (social insurance number, date of birth, hire date and choice of benefit program). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On September 26, 2018, an employee of the Organization was searching for internal policies when he noticed he was able to access an electronic folder titled "Human Resources" in the Organization's shared drive. • The employee immediately notified a Human Resources manager, who contacted IT. The proper accesses were restored the same day. • The Organization believes that the permission settings on the folder were inadvertently altered on August 8, 2018 when a new Human Resource employee requested permission to the folder. A contracted IT worker inadvertently unlocked the permissions so that the folder was potentially accessible to all employees who had access to the shared drive. • The Organization reported it has no evidence to indicate that any information contained in the folder was accessed or used by any unauthorized individual.
Affected individuals	The Organization reported that 44 active and inactive employees in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Investigated and determined this was an isolated incident. • Restored access permissions the same day the incident was discovered. • Obtained written confirmation from the employee who reported the incident, confirming he did not use, copy or disclose any information in the folder. • Endeavouring to obtain similar confirmation from the IT worker. • Reviewing and revising policies and technical protocols regarding changing permissions and providing additional training and awareness for applicable employees and staff, including in the IT department.
Steps taken to notify individuals of the incident	The Organization did not report notifying affected individuals.

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-trivial consequences or effects.	The Organization did not specifically identify the types of harm that might result from this breach. In my view, a reasonable person would consider that the contact, identity, employment and benefits information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation, and embarrassment.
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 "…does not believe that the incident gives rise to a real risk of significant harm, but has chosen to notify your Office out of an abundance of caution". The Organization also said that it "…has no evidence to indicate that any information contained in the Folder was accessed or used by any unauthorized individual. Further, there is no evidence to suggest that the IT worker who mistakenly altered the permissions settings of the Folder intended to access or misuse the personal information". In my view, a reasonable person would consider the risk of harm is decreased because the incident did not result from malicious intent, but rather was inadvertent. The employee who discovered the incident reported it and confirmed he did not use, copy or disclose any information in the folder. Despite the above, however, I am concerned that the Organization reported "there is no evidence to indicate that any information contained in the Folder was accessed or used by any unauthorized individual," rather than that the Organization reviewed audit logs and could confirm that there was no unauthorized access to information in the folder. The information may have been available for almost a month and a half.

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.

A reasonable person would consider that the contact, identity, employment and benefits information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation, and embarrassment. The risk of harm is decreased because the incident did not result from malicious intent, but rather was inadvertent. The employee who discovered the incident reported it and confirmed he did not use, copy or disclose any information in the folder.

Despite the above, however, I am concerned that the Organization reported "there is no evidence to indicate that any information contained in the Folder was accessed or used by any unauthorized individual," rather than that the Organization reviewed audit logs and could confirm that there was no unauthorized access to information in the folder. The information may have been available for almost a month and a half.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and **confirm to my office within 10 days of the date of this decision that it has done so.**

Jill Clayton
Information and Privacy Commissioner