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	Canon Medical Systems Canada Limited (Organization)
Decision number (file number)	P2018-ND-058 (File #008656)
Date notice received by OIPC	May 11, 2018
Date Organization last provided information	May 11, 2018
Date of decision	May 6, 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 those individuals whose personal information was collected in Alberta, 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • year of hire, • base annual salary (2017), • position, • home mailing address, and • Social Insurance Number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 30, 2018, and May 1, 2018, two employees notified the Organization that they had received letters mailed to their home addresses.

	• The letters appeared to be from the Ontario government, in connection with "Ontario's pay transparency legislation 2017", and included a spreadsheet listing other employees' personal information and a column comparing certain employees' pay relative to other employees with the same title. • The Organization investigated and found no evidence of any external intrusion into its relevant systems. The Organization believes that persons who historically had authorized access to the Organization's systems are the cause of the breach. • The Organization reported that it is aware of 15 employees who received the letters.
Affected individuals	The incident affected 126 employees and former employees, including 10 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation and followed up with current and former employees who had access to the human resources database in question. • Encouraging employees to monitor their banking accounts and financial statements and to consider activating credit monitoring services. • Advised employees that the information is outdated or inaccurate. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on May 1, 2018 and on May 5, 2018.
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 reported the "The fact that employees received the salary information of their co-workers has the potential to cause humiliation and damage to employee - employee and employee - employer relations. It is also possible that the harm could include identity theft or fraud, since it is possible that the breach includes social information numbers alongside the personal information that was breached." I agree with the Organization's assessment. A reasonable person would consider that the identity (social insurance number) and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation, embarrassment and damage to relationships.

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 "Based on the personal information disclosed in the letter, the likely harm (humiliation and damage to employee-employee and employee-employer relations) has already occurred". The Organization also reported that it believed identity theft and fraud were unlikely to result. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate extraction of personal information from a database) and has already been used to cause harm. The Organization cannot confirm whether the personal information will be used or disclosed in the future.

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 identity (social insurance number) and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation, embarrassment and damage to relationships. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate extraction of personal information from a database) and has already been used to cause harm. The Organization cannot confirm whether the personal information will be used or disclosed in the future.

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).

I understand the Organization notified affected individuals by email on May 1, 2018 and May 5, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner