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	Umicore Canada Inc. (Organization)
Decision number (file number)	P2015-ND-66 (File # 000053)
Date notice received by OIPC	December 18, 2014
Date Organization last provided information	December 18, 2014
Date of decision	October 30, 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 Alberta and 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: • name, • address, • date of birth, • telephone number, • postal code, • Social Insurance Number, • current salary, • performance reviews, • disciplinary action reports, • notification information, • medical absence reports, and • bonus payment information.

	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	• The Organization decommissioned and disposed of three computer servers. • An individual acquired the servers and found that one contained personal information of current and former employees of the Organization. • The individual anonymously reported the incident to the Organization on November 7, 2014. • An investigation into the incident was conducted. The servers were not recovered by the Organization. • The Organization reported that the individual agreed to wipe the servers before reusing them.
Affected individuals	A total of 108 individuals were affected by the incident.
Steps taken to reduce risk of harm to individuals	• An internal review was performed to determine if other computer servers containing personal information were insecurely disposed of by the Organization. • A review of the Organization's media disposal policy and procedure was performed. • Steps were taken to password-protect personal information on computer servers and consider encryption. • Free credit monitoring services were provided to individuals affected by the incident.
Steps taken to notify individuals of the incident	All affected individuals were directly notified by letter on December 17, 2015.
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 recognized that affected individuals may be at risk for identity theft, fraud, hurt, humiliation and reputational damage. I agree with the Organization. The personal information involved is highly sensitive as it includes identity and employment information. This information could be used to cause the harms of identity theft, fraud, hurt, humiliation and reputational damage. 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 due to the sensitivity of the personal information involved there is a real risk of significant harm to the affected individuals. In my view, the risk of harm is reduced because the incident did not result from malicious intent and the individual who acquired the servers reported the incident to the Organization and agreed to wipe the servers before reusing them. However, the Organization did not recover the servers and cannot confirm the personal information was destroyed, which increases the risk of 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 personal information involved sensitive identity and employment information. The risk of harm is reduced because the incident did not result from malicious intent and the individual who acquired the servers reported the incident to the Organization and agreed to wipe the servers before reusing them. However, the Organization did not recover the servers and cannot confirm the personal information was destroyed, which increases the risk of 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 the Organization notified affected individuals in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner