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	Hitachi Vantara Corporation (Organization)
Decision number (file number)	P2018-ND-146 (File #010030)
Date notice received by OIPC	October 16, 2018
Date Organization last provided information	October 16, 2018
Date of decision	November 15, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify affected individuals whose personal information was collected in Alberta.
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 data related to direct deposit information employees provided to the Organization for purposes of expense reimbursement, and may have included the following: • name, • number, • banking information (name and address bank, account number, routing number), • copy of a voided check in the employee's name, and/or • image of employee's signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported the information of three individuals was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization reported that it discovered that a third party may have gained access to an internal email account and that this "may have resulted in unauthorized access to the personal information of 3 Alberta residents." • The incident occurred on or after September 10, 2018 and ended October 4, 2018. • The breach was discovered on October 3, 2018 by an employee upon realizing that email had been sent from an internal email account by an unauthorized third party.
Affected individuals	The incident affected approximately 190 individuals, including 3 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the personal data from the impacted email account and changed internal processes to require that such data not be stored in an email account in the future. • Actively sought evidence that the information was actually viewed or used by the third party, and found no such evidence to date.
Steps taken to notify individuals of the incident	Affected individuals were not notified.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 that "It is possible that the unauthorized third party may use the affected information, such as digital image of signature or bank account or routing numbers, for malicious purposes such as financial fraud." I agree with the Organization's assessment. The financial information at issue could be used to cause the significant harms 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.	In assessing the likelihood of harm resulting from this breach, the Organization reported "We have identified limited possible harms because account access codes or passwords were not accessed as part of this incident." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for up to a month.

	Although the Organization reported that it has "sought evidence that the information was actually viewed or used by the third party, and found no such evidence to date", it appears the information was accessible to the intruder as the email account was used to send email. The Organization has not provided information to rule out the possibility that the unauthorized party will use the personal information at issue to cause harm.

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 as a result of this incident.

The financial information at issue could be used to cause the significant harms of identity theft and fraud. A reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for up to a month. Although the Organization reported that it has "sought evidence that the information was actually viewed or used by the third party, and found no such evidence to date", it appears the information was accessible to the intruder as the email account was used to send email. The Organization has not provided information to rule out the possibility that the unauthorized party will use the personal information at issue to cause harm.

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

Jill Clayton
Information and Privacy Commissioner