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	Nordstrom, Inc. (Organization)
Decision number (file number)	P2018-ND-142 (File # 010192)
Date notice received by OIPC	November 5, 2018
Date Organization last provided information	November 5, 2018
Date of decision	November 14, 2018
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 operates 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 information at issue could include: • name, • social insurance number, • pay card number, • checking account and routing number, • insurance provider information, • salary information, • date of birth, • address, and • telephone number. 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	• The breach involved a contract worker accessing employee data and downloading the data onto a USB key in violation of the Organization's security policies. • The key containing the data was retrieved from the contract worker and the Organization considers that the breach has been contained. • The breach happened on October 9, 2018 and was discovered the same day.
Affected individuals	The incident affected 519 Albertan employees.
Steps taken to reduce risk of harm to individuals	• Will offer the affected individuals information and resources to help them protect and monitor their information for any potential unauthorized activity. • Reported the breach to law enforcement, as well as the Privacy Commissioner of British Columbia and the Quebec Commission d'acces a l'information.
Steps taken to notify individuals of the incident	The Organization reported that "All affected individuals will be mailed a notification letter by November 6, 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 "Affected individuals are being counselled to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports." I agree with the Organization's assessment. The identity, contact, financial/employment and insurance information 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.	The Organization did not specifically assess the likelihood of harm resulting from this incident, but reported that "The key containing the data has been retrieved" and "There is no evidence at this time that data was shared or used inappropriately". Despite the fact the data has been retrieved and the breach contained, it is not clear whether this incident was the result of malicious intent or an inadvertent breach of policy. However, the Organization advised that it reported the incident to law enforcement, which suggests the contract worker may have had malicious or deliberate motivations.

	The Organization did not provide additional information beyond the statement that there is no evidence data was shared or used inappropriately. Without more information, I am unable to assess whether this is enough to mitigate potential significant 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 in this case.

The identity, contact, financial/employment and insurance information could be used to cause the significant harms of identity theft and fraud. Despite the fact the data has been retrieved and the breach contained, it is not clear whether this incident was the result of malicious intent or an inadvertent breach of policy. However, the Organization advised that it reported the incident to law enforcement, which suggests the contract worker may have had malicious or deliberate motivations. The Organization did not provide additional information beyond the statement that there is no evidence data was shared or used inappropriately. Without more information, I am unable to assess whether this is enough to mitigate potential significant harm.

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 reported that "All affected individuals will be mailed a notification letter by November 6, 2018." **The Organization is required to confirm to my office in writing within ten (10) days of the date of this decision that affected individuals were notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner