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	Data Facts, Inc. (Organization)
Decision number (file number)	P2019-ND-104 (File #012454)
Date notice received by OIPC	March 6, 2019
Date Organization last provided information	March 6, 2019
Date of decision	July 18, 2019
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 those 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 the following information: • name, • address, • driver's license number, • social insurance number, • passport 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	• On November 5, 2018, the Organization learned that an employee's email account was accessed by an unknown party. • That account contained personally identifiable information provided by clients for the purpose of conducting background checks.

	• The Organization reported it has no evidence to suggest that private information was misused; however, "…the possibility that emails and/or attachments in the account were viewed by the unauthorized party could not be ruled out." • On December 7, 2018, the Organization's investigation confirmed certain consumers' information was present in the account.
Affected individuals	The breach affected three (3) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately took steps to block access to the account by resetting passwords and hired a forensics firm to help investigate. • Re-educating employees on cyber best practices, including the use of a vendor to test employee responses to simulated common phishing campaigns. • Enhancing existing security measures related to authentication for remote email access, clearing deleted items folders, restricting the use of mailbox forwarding rules, forced password resets, and inbound and outbound filtering and blocking of emails potentially containing personally identifiable information. • Arranged for 12 months of credit monitoring and identity restoration services at no cost to the individual. • Reported breach to US and Canadian regulators.
Steps taken to notify individuals of the incident	Affected individuals in Alberta were notified by mail on February 15, 2019.
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 potential harms that might result from this incident, but reported that its notice to affected individuals "…includes guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the contact and identity 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.	The Organization did not specifically assess the likelihood of harm resulting from this incident, but reported it has no evidence to suggest that private information was misused. In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (unauthorized access).

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 and identity information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (unauthorized access).

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 that affected individuals in Alberta were notified by mail on February 15, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner