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	The Results Companies, LLC (Organization)
Decision number (file number)	P2021-ND-113 (File #016790)
Date notice received by OIPC	March 11, 2020
Date Organization last provided information	March 11, 2020
Date of decision	April 20, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual 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 the following information: • name, and • social security number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 13, 2019, the Organization discovered unauthorized access to an employee email account when a fraudulent wire transfer involving the Organization's corporate account was attempted. • The Organization investigated and determined that an employee email account had been used to facilitate the attempted wire transfer.

	• In the process of obtaining information to facilitate the attempted fraudulent wire transfer, it appears that the malicious actor may have accessed personal information without authorization. • The Organization reported the breach occurred on May 23, 2019.
Affected individuals	The incident affected 25,376 individuals, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Offered 12 months of credit monitoring and identity theft restoration services to the affected person. • Hired a consulting firm to disable all unauthorized access to the affected account. • Engaged third party forensics firms to identify and eliminate any vulnerabilities and to increase the existing security of the email environment. • Enhanced the existing security of its email environment. • Implemented additional security measures such as multifactor authentication, restricted administrative access, enhanced alerting on new account creation and privilege elevation, enhanced event logging and disabled functions such as auto-forwarding.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 11, 2020.
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's report of the breach said that it "...is offering the affected individual complimentary credit monitoring and identity theft restoration services". In my view, a reasonable person would consider that the 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 provide its assessment of the likelihood of harm resulting from this breach, but reported: *After discovering the matter, [the Organization] immediately hired a consulting firm who disabled all unauthorized access to the affected account. In addition, [the Organization] engaged third party forensics firms to identify and eliminate any vulnerabilities and to increase the existing security of the email environment. [The*

	Organization] has also taken a number implementation of the following additional security measures: • *Enabled multi-factor authentication;* • *Restricted administrative access;* • *Enhanced alerting on new account creation or privilege elevation;* • *Enhanced event logging; and* • *Disabled certain functions, and blocked certain rules, such as auto-forwarding.* *In addition, [the Organization] is offering the affected individual complimentary credit monitoring and identity theft restoration services through ID Experts. All appropriate U.S. and Canadian regulatory authorities/data protection authorities have been notified of the incident.* In my view, a reasonable person would consider the likelihood of harm is increased as the breach resulted from malicious action (deliberate, unauthorized access and attempted fraud). It appears the email account was compromised for over 2.5 months before the breach was detected.

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 information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is increased as the breach resulted from malicious action (deliberate, unauthorized access and attempted fraud). It appears the email account was compromised for over 2.5 months before the breach was detected.

I require the Organization to notify the affected individual 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 letter dated March 11, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner