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	Rightway Immigration and Education Services (Organization)
Decision number (file number)	P2021-ND-318 (File #021330)
Date notice received by OIPC	May 21, 2021
Date Organization last provided information	May 21, 2021
Date of decision	March 7, 2022
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 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 operates in India and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • full name, • postal address, • email address, • telephone number, • government identification documents (including passport information, immigration documentation and tax IDs), • social insurance number, • financial information (employees), • date of birth, and • student identification information. 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 January 17, 2020, The Organization discovered suspicious activities in its email accounts. • The Organization determined that threat actors accessed two mailboxes frequently, between September 17, 2019 and January 17, 2020. A third mailbox was accessed twice, on September 21 and 23, 2019. The Organization's investigation also found that four links had been created for document transfers from the account. • The Organization reported, "evidence was not available to identify which emails were accessed" or "which files were contained in the links, nor whether the links were accessed by the threat actors."
Affected individuals	The incident affected 1,292 Canadians, including 162 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled and stopped using the compromised email account. • Changed all passwords and implemented a password rule where passwords are changed every 30 days. • Implemented multi-factor authentication for its accounts. • Retained the services of an external forensic firm to perform a data mining exercise and to identify the personal information potentially affected as well as contact information for affected individuals. • Informed business partners of the incident and the change of email address in order to reduce the risk of harm. • Notified affected individuals and recommended they remain vigilant about potential risks of a phishing campaign • Offered twelve (12) months credit monitoring services at no cost to the affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and mail on April 29, 2021.
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 "Considering the type of information at issue, the potential harms may include identity theft, fraud, financial loss and email phishing." I agree with the Organization's assessment. A reasonable person would consider that contact, identity, and financial information at issue could be used to cause identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 it… *… considers that there is a risk of harm. While there was no evidence of data exfiltration, the two mailboxes were accessed a number of times and the organization could not identify the specific emails that were potentially accessed to rule out this risk.* *The organization is not aware of any misuse of personal information with the exception of the three clients initially affected by the third party's impersonation of the organization's employees to initiate fraudulent money transfers.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (impersonation, phishing). The Organization reported that although there was no evidence of data exfiltration, it "could not identify specific emails that were potentially accessed…". The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, it appears the email accounts were exposed for approximately four (4) months.

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 contact, identity, and financial information at issue could be used to cause identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (impersonation, phishing). The Organization reported that although there was no evidence of data exfiltration, it "could not identify specific emails that were potentially accessed…". The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, it appears the email accounts were exposed for approximately four (4) months.

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 the Organization notified affected individuals by email and mail on April 29, 2021 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner