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	Real Estate Council of Alberta (Organization)
Decision number (file number)	P2020-ND-108 (File #013085)
Date notice received by OIPC	August 30, 2019
Date Organization last provided information	October 18, 2019
Date of decision	September 24, 2020
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 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name, • social insurance number, • financial information (credit card and banking information), • airline rewards number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 20, 2019, an unknown individual gained unauthorized access to an employee email account through a phishing attack. • The unknown individual set up an automatic forwarding rule such that all incoming emails were forwarded to a third party email address that appears to have originated from outside of Canada. The email address is unknown to the Organization.

	• The Organization's IT department determined that 1,180 emails were forwarded to the external email address between June 20, 2019 and August 27, 2019. Of those, an estimated 835 were identified as containing personal information. • The breach was discovered on August 27, 2019 during a routine review of Microsoft Office 365.
Affected individuals	The incident affected four (4) individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled the affected account, removed the forwarding rule and changed the compromised password. • Deployed two factor authentication for the affected staff member, and will roll this out to all staff members. • Reviewing cybersecurity procedures and implemented additional security configurations in Office 365. • Providing additional cybersecurity training for all staff. • Installed intrusion detection software. • Provided guidance to affected individuals regarding measures to protect their personal information. • Offering credit monitoring services to those affected.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and in writing between September 25 and 26, 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 initially reported that the possible harms that may occur as a result of the breach are "Embarrassment, hurt or humiliation; damage to reputation or relationships; identity theft; fraud; email phishing or spear-phishing attacks; loss of employment, business or professional opportunities". In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to 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 reported: *It is likely that there is a real risk of significant harm to some of the individuals whose personal information was forwarded to the external email address.* The Organization identified a number of factors contributing to this assessment, including the sensitivity of the information at issue, the likelihood of malicious intent, the length of time the external email forward was in place. The Organization also noted

	that “no evidence has come to light of any harm actually occuring [sic]”. 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 (phishing). The unauthorized party had access for up to 9 weeks. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach.

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 and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 (phishing). The unauthorized party had access for up to 9 weeks. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach.

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 the affected individuals by telephone and in writing between September 25 and 26, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner