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	Barr Picard Law (Organization)
Decision number (file number)	P2021-ND-027 (File #013423)
Date notice received by OIPC	October 7, 2019
Date Organization last provided information	January 27, 2020
Date of decision	February 23, 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 those individuals 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 all or some of the following information: <u>Type 1:</u> • full name, • property address purchased and sold, • purchase price for properties, • mortgage amounts, • mortgage number for the property in question, • copy of voided cheque and debit card, and • cheque from opposing counsel's client. <u>Type 2</u>: • full name, and • address of property sold. 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 October 1, 2019, the Organization discovered that a staff member's email account was compromised and messages received by this email account had been forwarded externally. • The Organization said that only incoming emails were affected by the email-forwarding rule. • The breach occurred on or about September 17, 2019 to October 29, 2019. • The Organization reported that the documents involved did not include completed mortgage documentation and the information involved is publicly available through the land titles registries. • The Organization discovered the incident when it received a scam email, directing it to deposit funds.
Affected individuals	The incident affected 181 residents in Alberta.
Steps taken to reduce risk of harm to individuals	• Changed the staff's email account. • Compiled list of affected individuals. • Informed affected individuals to remain vigilant about suspicious activity and check credit reports. • Offered a 12-month subscription for credit monitoring service to individuals with Type 1 information affected by the breach.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 27, 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 that "If those emails contain financial information, that can be used by a third party." In my view, a reasonable person would consider that the contact and financial 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.	In its notification to affected individuals, the Organization said "The information involved is available to the public through the land titles registries and we believe that there is very little risk of harm to you as a result of this breach." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 6 weeks. The

	breach was discovered when the Organization received a scam email, directing it to deposit funds.

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 financial information could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (phishing and email forwarding rule). It appears the email account was exposed for approximately 6 weeks. The breach was discovered when the Organization received a scam email, directing it to deposit funds.

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 in an email on January 27, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner