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	Mitten Building Products (Organization)
Decision number (file number)	P2021-ND-022 (File #016525)
Date notice received by OIPC	July 24, 2020
Date Organization last provided information	July 24, 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 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 all or some of the following information: • name, • address, and • financial account information (bank account number and routing 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 25, 2020, the Organization discovered that between August 31, 2019 and November 10, 2019, an unauthorized person accessed certain of the Organization's employees' email accounts at various times.

	• The Organization was not able to determine which emails and attachments, if any, were accessed by the unauthorized person, but conducted a comprehensive review of the contents of the email accounts. • To date, the Organization has no evidence of any misuse of the information as a result of this incident.
Affected individuals	The incident affected 91 individuals, including one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Secured the email accounts, launched an investigation, and engaged a cybersecurity firm to assist. • Recommended that individuals closely review their financial account statements for any unauthorized activity. • Established a dedicated call center for individuals to obtain information regarding the incident. • Implementing additional safeguards and technical security measures.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on July 27, 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 reported the possible harms that may occur, as a result of the breach as "None." However, the Organization's notice to affected individuals said "We remind you it is advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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 provide its assessment of the likelihood of harm resulting from this incident, but reported it "… is recommending that individuals closely review their financial statements for any unauthorized activity." 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 (deliberate intrusion into an employee's email account). The Organization said it has no evidence that the information was misused; however, the compromised information may well have continuing value over

	time. Further, the information may have been exposed for approximately 2 ½ 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 the contact and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. 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 (deliberate intrusion into an employee's email account). The Organization said it has no evidence that the information was misused; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately 2 ½ months.

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 the affected individual by letter on July 27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner