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	Ply Gem Residential Solutions (Organization)
Decision number (file number)	P2020-ND-096 (File #016526)
Date notice received by OIPC	July 27, 2020
Date Organization last provided information	July 27, 2020
Date of decision	September 3, 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's head office is located in North Carolina, USA, 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: • name, • date of birth, • Social Insurance Number, • financial account information, • health insurance information, and • limited clinical or treatment information. 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 an unauthorized individual may have accessed certain employees' email accounts at various times between July 26, 2019 and November 18, 2019.

	• The Organization investigated and was not able to determine which email accounts and attachments, if any, were accessed. • The Organization conducted a review of the contents of the email accounts. • The Organization has no evidence to date of any misuse of the information.
Affected individuals	The incident affected 67,563 individuals, including 1,802 in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the email accounts. • Launched an investigation. • Engaged a cybersecurity firm. • Implemented additional safeguards to protect the security of information in its systems. • Established a call centre for affected individuals to contact with questions or concerns. • Offered a complimentary, one-year membership for credit monitoring and identity theft protection. • Providing guidance related to protecting against identity theft and fraud. • Providing additional date security training to employees. • Reported the incident to the FBI.
Steps taken to notify individuals of the incident	The affected individuals in Alberta were notified by letter sent 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 stated that "Stolen Social insurance numbers can be used to commit identity theft." In my view, a reasonable person would consider that the identity, financial and insurance information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all 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 is "…offering eligible individual a complimentary, one-year membership to Transunion credit monitoring and identity theft prevention. To further diminish the likelihood of harm, Ply Gem is recommending that the individuals involved closely review their financial and/or medical 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 employees' email accounts). The Organization said it has no evidence that the information was misused or specifically targeted; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately four 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 identity, financial and insurance information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all 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 (deliberate intrusion into employees' email accounts). The Organization said it has no evidence that the information was misused or specifically targeted; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately four 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 letter sent on July 27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner