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	American Frame Corporation (Organization)
Decision number (file number)	P2021-ND-248 (File #020915)
Date notice received by OIPC	February 9, 2021
Date Organization last provided information	May 12, 2021
Date of decision	December 1, 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 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, • mailing address, • social security number, and/or • credit card information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 1, 2020, the Organization was the subject of a cyberattack involving the encryption of data and a ransom demand in exchange for decryption (ransomware). • The Organization reported that personal information was exposed and may have been accessed during the attack.

Affected individuals	The incident affected 30,502 individuals, including 2 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated the incident with the assistance of a forensic specialist. • Notified police. • Reviewed and altered security practices, policies, and tools. • Reviewed and altered information life cycle management. • Offered credit monitoring and identity theft protection services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on or about January 14, 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 "Individuals' personal information may be used unlawfully." In my view, a reasonable person would consider that the contact, identity (social security number), and/or financial information at issue could be used to cause the significant harms of fraud, identity theft, or negative effects on a credit record.
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 "There is a medium to high probability that individuals' personal information was compromised." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, encryption of records, and demand for ransom payment). The Organization reported that personal information was exposed and may have been accessed during the attack.
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, identity (social security number), and/or financial information at issue could be used to cause the significant harms of fraud, identity theft, or negative effects on a credit record. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, encryption of records,	

and demand for ransom payment). The Organization reported that personal information was exposed and may have been accessed during the attack.

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 mail on January 14, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner