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	Windward Software Systems Inc. (Organization)
Decision number (file number)	P2021-ND-072 (File #017685)
Date notice received by OIPC	October 7, 2020
Date Organization last provided information	November 20, 2020
Date of decision	March 9, 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 the following information collected in Alberta: • name, • address, • date of birth, • social insurance number, and • bank account information. 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 September 1, 2020, the Organization was subject to a cyberattack, resulting in the exfiltration of records and the unauthorized encryption of some organizational infrastructure.

	• The incident was discovered the same day, September 1, 2020; however, data exfiltration was confirmed 8 days later on September 9, 2020 after records were discovered on the dark web.
Affected individuals	The incident affected 148 individuals, of which 2 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Obtained the assistance of cybersecurity and forensic IT experts. • Notified law enforcement. • Turned off "single-factor authentication VPN." • Increased password complexity requirements. • Reset all passwords. • Updated software, including servers, firewalls, and network equipment firmware. • Enabled additional security software functionality. • Reviewed security and cybersecurity policies and procedures.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and/or email on September 9, 2020. A supplementary notice was provided to the second impacted Albertan by email on November 12, 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 "...there are potential risks of identity theft, fraud and financial loss and embarrassment for the individual affected in Alberta." I agree with the Organization's assessment. A reasonable person would consider that the identity, contact, and financial information at issue could be used to cause the harms of identity theft, fraud, financial loss or negative effects on a credit record. These are 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 reports: *[T]he likelihood that harm could result is high … because sensitive data was posted on the dark web.* *[T]he likelihood that harm could result is moderate for the rest of the affected individuals. While [the Organization] has no evidence that the personal information at issue has been misused by the external actor, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes of identity theft and*

	fraud. The fact that the incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result. In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an third party who demanded ransom payment and released the exfiltrated records on the dark web. Further, the Organization did not report removing the records from the dark web. The lack of reported misuse to date does not mitigate against harms occurring in the future.

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, contact, and financial information at issue could be used to cause the harms of identity theft, fraud, financial loss or negative effects on a credit record. These are 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 third party who demanded ransom payment and released the exfiltrated records on the dark web. Further, the Organization did not report removing the records from the dark web. The lack of reported misuse to date does not mitigate against harms occurring in the future.

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 telephone and/or email on September 9, 2020, and by email on November 12, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner