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	Haws Corporation (Organization)
Decision number (file number)	P2019-ND-189 (File #013308)
Date notice received by OIPC	May 22, 2019
Date Organization last provided information	May 22, 2019
Date of decision	December 13, 2019
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, • address, and • Social Security number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 1, the Organization experienced a ransomware attack. The breach was discovered the same day when employees were unable to access their systems. • The Organization immediately engaged computer experts to determine what the impact was to the system and to negotiate with the threat actor.

	• A forensic investigation was completed on or about March 26, 2019, but was unable to conclude whether sensitive personal information was accessed by the threat actor.
Affected individuals	The incident affected approximately 149 individuals.
Steps taken to reduce risk of harm to individuals	• Offered 12 months of credit monitoring and identity theft restoration service to affected individuals. • Reviewed company policies and procedures to ensure that security measures are in place to prevent reoccuring incidents and implemented various security recommendations made by cyberforensic expert to improve system security.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 9, 2019.
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 possible harms that might result from this incident include "Identity theft, credit fraud". In my view, a reasonable person would consider the contact and identity information at issue 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.	The Organization reported "We have received no indication to date that employee information has been misused to date. We believe there is a low-likelihood that harm will result from this incident." 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 action, ransom demand). The Organization's investigation was "unable to conclude whether sensitive personal information was accessed by the threat actor". The lack of reported misuse of the information to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.
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 the contact and identity information at issue could be used to cause the significant harms of identity theft, and fraud. The likelihood of harm is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action, ransom demand). The Organization's investigation was "unable to conclude whether sensitive personal information was accessed by the threat actor". The lack of reported misuse of the information to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

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 affected individuals were notified by letter on May 9, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner