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	Home Hardware Stores Limited (Organization)
Decision number (file number)	P2021-ND-199 (File #020130)
Date notice received by OIPC	March 11, 2021
Date Organization last provided information	March 11, 2021
Date of decision	October 18, 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 operates in Alberta 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: <u>Current and former employees, and minors</u> • name, • physical address, • email address, • telephone number, • date of birth, • gender, • social insurance number, • other government issued identification, • emergency contact information, • income, • benefits, • deductions, • garnishments, • banking information, • hire date, • termination date, • severance payment, • performance review,

	• resume, • interview notes, • attendance record, • disciplinary investigations, and • medical leave information. <u>Current and former business partners and Dealer-Owners</u> • business name, • email, • date of birth, • social insurance number, • credit application information, • payment amounts, • payment processor ID, • financial institution information, and • signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies. The Organization also reported that some of the personal information was from "business partners" and "Dealer-Owners" including business names and email addresses. "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As such, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 18, 2021, the Organization's Information Technology (IT) staff found maliciously encrypted files while troubleshooting IT infrastructure that was not operating properly. • Investigation of the incident determined that suspicious network activity began on February 12, 2021, when an unauthorized party appeared to be logging in and testing credentials. The unauthorized party deployed "hacking tools" on February 16 and 17, 2021. Lastly, a ransomware attack was deployed on February 18, 2021. Attempts to attack the environment continued for several days, but were blocked by the Organization. • The Organization reports that the unauthorized third party copied and removed data from their systems.
Affected individuals	The incident affected 5,242 Canadian individuals, including 11 minors, and 856 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation with the assistance of forensic IT experts. • Offered 60 months of identity theft and credit monitoring services to individuals at risk of identity theft or fraud. • Conducting a review of security and cybersecurity measures to improve safeguards. • Conducting a review of cybersecurity and privacy policies and procedures. • Notified police.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter between March 2, 2021 and March 5, 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: *For current and former employees, it is [the Organization's] assessment that since the potential personal information involved in the Incident includes financial, contact / identification information, human resource data, there are potential risks of identity theft, fraud and financial loss, phishing and embarrassment.* *For current and former business partners and Dealer-Owners, it is [the Organization's] assessment that since the potential personal information involved in the Incident includes financial and identification information there are potential risks of identity theft, fraud and financial loss.*

	The specified harm noted above, assuming they occur, are significant. In my view, a reasonable person would consider that the contact, identity, employment, and financial information could be used to cause the harms of identity theft, fraud, financial loss, and negative affects on a credit record. Health (medical leave information) and employment information (interview notes, performance reviews, garnishments, and disciplinary investigations) could also be used to cause the harms of damage to reputation or relationships, loss of business or professional opportunities, and embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to the above. 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... *.. of the view that the likelihood that harm could result is low to moderate. While [the Organizaiton] has no evidence confirming that the personal information at issue has been compromised or misused by the external unauthorized actor, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes identified above.* *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.* I accept 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 an unauthorized third party (deliberate intrusion and deploying malicious payloads including ransomware). A lack of evidence that personal information has been misused is not a mitigating factor against future harms.
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, employment, and financial information could be used to cause the harms of identity theft, fraud, financial loss, and negative affects on a credit record.

Health (medical leave information) and employment information (interview notes, performance reviews, garnishments, and disciplinary investigations) could also be used to cause the harms of damage to reputation or relationships, loss of business or professional opportunities, and embarrassment, hurt or humiliation.

Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to the above. 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 unauthorized third party (deliberate intrusion and deploying malicious payloads including ransomware). A lack of evidence that personal information has been misused is not a mitigating factor against future harms.

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 email or letter between March 2, 2021 and March 5, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner