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	Calgary House of Cars 6 Inc. (Organization)
Decision number (file number)	P2021-ND-217 (File #019539)
Date notice received by OIPC	December 11, 2020
Date Organization last provided information	September 27, 2021
Date of decision	November 3, 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 these individuals 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>Employees:</u> • full legal name, • home address, • home email address, • home telephone number, • social insurance number, • terms and conditions of employment, • employee discipline, if any, • information relating to benefits entitlement, • banking information (i.e. a void cheque), and • driver's license information. <u>Customer:</u> • full legal name, • home address, • home email address, • home telephone number, • driver's license information, • employment information, and

	• banking and financial information (i.e. copies of all lending documents, including credit application and the contract between customer and financial institution). The Organization reported, "it is believed that the personal information of only one customer has been lost." 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 December 7, 2020, the Organization discovered that intruder(s) gained access to their office and seized a desktop computer, as well as hard copies of certain files. • The computer is password-protected and is being monitored via the Organization's system. The Organization reported that it would be necessary for any illicit user to hack the device's password as well as several further levels of encrypted software in order to access information on the system; further, all relevant passcodes were changed. • The Organization reported that since it is dependent largely upon a hard-copy filing system, the amount of personal information accessible through the computer, even if successfully hacked, is small. • As of the date of the breach report, the intruders have not yet been apprehended and the computer has not been activated or used to log on to the system.
Affected individuals	The incident affected approximately 12 to 15 individuals.
Steps taken to reduce risk of harm to individuals	• Uploaded all employee and customer information to a secure server. • Reviewed and strengthened encryption policies for all company devices, including any desktops, laptops, and cellphones. • Reviewed the scope and nature of the services implemented by the third-party security services provider in order to ensure optimally guarded against similar threats in the future. • Reviewed privacy and record management policies to ensure they address administrative, technical, and physical safeguards to mitigate the loss of records in the future. • Reported the incident to the Calgary Police Service and an investigation is ongoing.

Steps taken to notify individuals of the incident	The affected individuals were notified by telephone and email and by letter dated December 10, 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, *Possible harms to the individuals affected by the Breach include identity theft, unauthorized access, use, or disclosure of sensitive information (employment, professional, financial history) that may cause embarrassment. Further, the loss banking and financial information could lead to unauthorized purchases or fraudulent activity.* *In all the relevant circumstances, and particularly in light of the fact that the Breach occurred as a result of criminal activity involving a physical breach of…premises, we believe that there is a real risk of significant harm.* I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The employment and financial history could be used to cause the significant harm of humiliation and embarrassment.
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 "There is currently no evidence of any unauthorized use of this information." In its notification to the affected individual, the Organization stated… *...we recommend that you change important passwords (particularly those relating to online banking or shopping), contact your financial institution(s) in order to alert them to the potential for fraudulent transactions, and take whatever further steps you think prudent in the circumstances.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization reported, "There is currently no evidence of any unauthorized use of this information", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. The information has not been recovered.

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 and identity information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The employment and financial history could be used to cause the significant harm of humiliation and embarrassment. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization reported, "There is currently no evidence of any unauthorized use of this information", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. The information has not been recovered. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individuals were notified by email and by letter on December 20, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner