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	New Horizons Car & Truck Rentals Inc., operating as Discount Car and Truck Rentals (Organization)
Decision number (file number)	P2021-ND-182 (File #019705)
Date notice received by OIPC	March 1, 2021
Date Organization last provided information	May 25, 2021
Date of decision	September 2, 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 owns the brand "Discount Car and Truck Rentals" in Alberta. 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, • driver's licence number, • passport number, • date of birth, • email address, • telephone number, • full or partial postal address, • full or partial payment card number, • payment card expiry date, • auto insurance policy and claim information, • financial account number, • financial routing number, • copy of personal cheque, • information relating to collections claim(s), • consumer credit report, • employee compensation 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 the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 20, 2021, the Organization was the victim of a cyber-attack. • The breach was detected 19 days later on February 8, 2021, when the Organization detected ransomware on its systems. • The Organization's investigation determined that, in addition to encrypting some servers, the attacker may have exfiltrated unstructured email and email attachment data from some of the Organization's systems. • The root cause of the incident was not reported by the Organization.
Affected individuals	The incident affected approximately 18,485 individuals.
Steps taken to reduce risk of harm to individuals	• Engaged its incident response and began isolating impacted systems. • Engaged a cyber security firm to assist with containing and investigate the breach. • Took steps to secure the network environment. • Restored systems at an offsite facility. • Implemented additional vulnerability scanning, endpoint detection, and applied critical patching. • Changed all system passwords. • Reported the incident to law enforcement. • Offered credit monitoring to certain affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter or email on May 8, 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: *In the Company's view, a listing of potential harms (e.g., a potential use of an email address for phishing) would be speculative, and certainly no indication of any "real risk of significant harm" to Affected Individuals.* Despite this, the Organization's notices to affected individuals included the following:

	As always, please be cautious of any unsolicited communications that ask you to provide your personal information electronically, and avoid clicking on links or downloading attachments from suspicious emails. As well as the following: *As a precautionary measure, we have arranged with Equifax to provide you with a two-year subscription to the Equifax Complete Premier Plan, a credit monitoring service … With the Equifax Complete Premier Plan you can:* *Help minimize exposure. Your Equifax plan includes internet scanning and dark web monitoring.* *Help reduce financial risk with up to $50,000 of identity theft insurance.* *In addition, upon your request and at no cost, Equifax can place a fraud alert on your credit file. This is a notice that is placed on your credit report that alerts lenders and other companies who may extend you credit that your personal information may have been compromised.* In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft, fraud, or financial loss. Collections claims and credit reports, in combination with contact, identity, and financial information, could be used to cause the harms of identity theft, fraud, negative effects on a credit record, or potentially embarrassment, hurt and humiliation. Email addresses could be used for phishing, increasing 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: *[Given] the highly unstructured state of the data, and the non-sensitive nature of the vast majority of the data in the affected records, the Company determined that there is a very low risk of actual harm to Affected Individuals arising from this incident.* In my view, the likelihood of harm resulting from this incident may be reduced given the unstructured state of the data. Despite this, the likelihood of harm resulting from the incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion, deployment of ransomware). Further, the Organization

	did not rule out the possibility that personal information was exfiltrated.

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, and financial information at issue could be used to cause the harms of identity theft, fraud, or financial loss. Collections claims and credit reports, in combination with contact, identity, and financial information, could be used to cause the harms of identity theft, fraud, negative effects on a credit record, or potentially embarrassment, hurt and humiliation. Email addresses could be used for phishing, increasing vulnerability to the above. These are all significant harms.

The likelihood of harm resulting from this incident may be reduced given the unstructured state of the data. Despite this, the likelihood of harm resulting from the incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion, deployment of ransomware). Further, the Organization did not rule out the possibility that personal information was exfiltrated.

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 letter or email on May 8, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner