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	Avis Budget Group, Inc. (Organization)
Decision number (file number)	P2017-ND-139 (File #006497)
Date notice received by OIPC	September 7, 2017
Date Organization last provided information	September 7, 2017
Date of decision	October 3, 2017
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 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, • mailing address, • telephone number, and • email address. 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	• Between August 22-23, 2017, the Organization detected what it believes to have been a brute force/ dictionary intrusion by an unauthorized third party against the Organization's application program interface of Avis Preferred (a rental mobile application that allows customer to create user accounts that, among other features, allows customers to book rentals).

	• As a result of this event, the Organization believes that an unauthorized third party may have been able to access the information at issue. • The Organization is unable to confirm that the information was accessed, and has not received any reports of misuse of the information with respect to its rental services, nor any reports of phishing activity using the contact information.
Affected individuals	The incident affected information of 218 Canadian residents, of whom 44 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Initiated response procedures and locked the potentially affected application accounts, requiring users to reset their passwords. • Conducted a full investigation and is reviewing and analyzing the findings and will implement any lessons learned to mitigate future similar events (including enhanced detection capabilities). • Monitoring affected accounts for any suspicious activity involving its rental services.
Steps taken to notify individuals of the incident	On September 6, 2017, the Organization began notifying all Canadian customers by email. Where email is not possible, affected individuals were notified by letter or telephone.
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 "The information that was capable of being accessed is of low value to the unauthorized third party. In intrusions like this, the motivation is more often to obtain payment card information and/or to initiate a rental and then steal the vehicle from Avis." In my view, the contact and email information at issue could be used to make unsolicited telephone calls/send unsolicited mail, and for phishing. In previous breach notification decisions I have found phishing to be a significant harm.
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 seems unlikely that there is any real risk of significant harm, since the likely motivation was to obtain payment card information and/or to defraud [the Organization] by renting and stealing vehicles". In my view, the likelihood of significant harm (phishing) resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The Organization can only speculate as to the motive and intentions of the unauthorized third party.

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. The contact and email information at issue could be used to make unsolicited telephone calls/send unsolicited mail, and for phishing. In previous breach notification decisions I have found phishing to be a significant harm. The likelihood of significant harm (phishing) resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The Organization can only speculate as to the motive and intentions of the unauthorized third party. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified all Canadian customers by email, letter or telephone, beginning September 6, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner