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	car2go Canada Ltd (Organization)
Decision number (file number)	P2017-ND-42 (File #005016)
Date notice received by OIPC	February 21, 2017
Date Organization last provided information	February 21, 2017
Date of decision	March 6, 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 federally incorporated and operates in Alberta. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • date of birth, • address, • primary telephone number, • email address, and • driver's license number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some or all of the information about Albertans was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about December 23, 2016, the Organization noted fraudulent activities within its systems after some members reported unauthorized activities on their accounts. The Organization also noticed changes to member data and requests for new numbers, as well as unusual activity concerning vehicle use and trip duration. • The Organization investigated and found there had been a brute force attack against its system in late December, whereby unauthorized third parties accessed member accounts using lists of email/password combinations to log into the systems and verify valid matches for accounts. • The Organization confirmed that the attacker(s) knew the credentials of the members or used commonly-used passwords (e.g. "password," or "12345") to gain access to accounts, and that the incident was not due to any data leaks or weakness in the Organization's systems. The unauthorized third parties logged-in to accounts and then requested the PIN in order to drive and use the Organization's cars.
Affected individuals	The incident affected 27 Alberta members.
Steps taken to reduce risk of harm to individuals	• Initiated an internal investigation. • Set up random passwords for affected members, disabled account access, shut down open rentals when able to do so, and notified the affected members. • Reported the incident to law enforcement. • Updated its system and created a new authentication process. • Reminded members to use strong and unique passwords. • Enhancing ability to improve the detection of these types of brute force attacks, and will upgrade its system.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone between December 27, 2016 and January 14, 2017.
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 "While … members' accounts did not contain financial information, once the accounts were accessed, fraudsters could use the members' information to request a PIN and drive [one of the Organization's] cars. Since the personal information available within the member's account in …[the] system include the name and address of the members, combined with the date of birth and a unique number (driver's license number), it was determined that such information could also potentially be used for fraudulent purposes (i.e. including identity theft)."

	I agree with the Organization's assessment. Identity (date of birth, driver's license number), contact and profile information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. These are 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 did not specifically assess the likelihood of harm resulting from this incident, but advised affected individuals to reset their passwords and "monitor their personal account statements and credit reports to detect any suspicious or unauthorized activity." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (deliberate intrusion). Further, the information was used for fraudulent purposes (vehicle theft and theft of services, unauthorized changes to member accounts).

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. Identity (date of birth, driver's license number), contact and profile information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. These are significant harms. The likelihood of harm is increased because the personal information was compromised due to malicious action (deliberate intrusion). Further, the information was used for fraudulent purposes (vehicle theft and theft of services, unauthorized changes to member accounts).

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 affected individuals by telephone between December 27, 2016 and January 14, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner