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	Audi Canada Inc., and Volkswagen Group Canada Inc. (Organization)
Decision number (file number)	P2021-ND-333 (File #021645)
Date notice received by OIPC	June 17, 2021
Date Organization last provided information	December 10, 2021
Date of decision	March 10, 2022
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 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, • personal mailing address, • business mailing address, • email address, • telephone number, and • information about purchased or leased vehicle, such as vehicle identification number, make, model, year, color, and trim packages. Some of this information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the personal information appears to be business contact information, which 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 e-mail address, business fax number and other similar business information".

	Section 4(3)(d) of PIPA says that the Act does not apply to "the collection, use or disclosure of an individual's business contact information if the collection, use or disclosure, as the case may be, is 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 and for no other purpose." As such, the information is not excluded from the Act and PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On March 10, 2021, the Organization was notified that data relating to its customers was in the custody of an unauthorized third party. • An investigation determined that "at some point between August 2019 and May 2021," one of the Organization's vendors inadvertently set "cloud containers containing [the Organization's] data to open permissions". The Organization believes "the threat actor intentionally took the data at issue".
Affected individuals	The incident affected 3.3 million individuals, including 13,733 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated the incident. • Retained cybersecurity and data analytics consultants. • Engaged an external forensics service provider. • Secured the records. • Worked with the vendor to address the matter, including a review of the vendor's security practices and procedures. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter between June 16 and 22, 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 that "The main harm resulting from this information being obtained by an unauthorized party is that it will be used for phishing attempts to obtain more sensitive information." I agree with the Organization's assessment. A reasonable person would consider that the contact information (email addresses) at issue could be used for the purposes of phishing, increasing affected individuals' risk the significant harm of fraud and possibly identity theft.
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: *For the following reasons, [the Organization] does not believe that there is a risk of significant harm, and are providing this Privacy Breach Report Form voluntarily to the OIPC:* *- The personal information exposed does not appear to be particularly sensitive (as it did not contain personal financial information nor did it contain government identification of individuals).* *- In terms of personal data points, not every data point was available for each customer, as some customers did not have complete information profiles.* *- Our client believes that this harm can be reduced by alerting individuals to the risk and reminding them to be alert and not to provide information to any person or entity claiming to be [the Organization].* *- [The Organization is] taking a variety of steps designed to reduce the likelihood/risk of harm to individuals (as described below).* On December 9, 2021, the Organization further reported: *The vendor has indicated that the containers with personal information are generally set to private permissions by default, and the vendor therefore believes the incident likely resulted from an isolated human error where the default settings for these containers were manually overridden.* *As noted, we believe the vendor misconfigured the container permissions inadvertently (not intentionally). We*

	believe the threat actor intentionally took the data at issue, but do not know whether this data was targeted in particular. In my view, a reasonable person would consider that the likelihood of harm may be decreased because the personal information was disclosed without authorization due to human error (misconfiguration of a technical safeguard). Nonetheless, the exposed records were deliberately accessed without authorization by a "threat actor" whose intent is unknown. Further, the personal information may have been exposed for nearly 2 years.
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 information (email addresses) at issue could be used for the purposes of phishing, increasing affected individuals' risk the significant harm of fraud and possibly identity theft. The likelihood of harm may be decreased because the personal information was disclosed without authorization due to human error (misconfiguration of a technical safeguard). Nonetheless, the exposed records were deliberately accessed without authorization by a "threat actor" whose intent is unknown. Further, the personal information may have been exposed for nearly 2 years. 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 and letter between June 16 and 22, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner