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	Mercedes-AMG GMBH (Organization)
Decision number (file number)	P2022-ND-018 (File #022384)
Date notice received by OIPC	October 13, 2021
Date Organization last provided information	October 13, 2021
Date of decision	April 21, 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 the 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's head office is in Germany. 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 the following information: • username, • password, and • email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 21, 2021, the Organization was made aware that personal data files relating to users of its 'Private Lounge' service was being offered for sale on a web forum. • The Private Lounge is an internet community platform established and provided by the Organization for owners of Mercedes-AMG vehicles, who could register to join the Private Lounge via an online registration process.. • An external security researcher reported the sale of the data.

	• The web forum post claims to have details of approximately 99,000 customer records for the Private Lounge service dating from 2019 and earlier. • The incident resulted from a compromise of data sets relating to Private Lounge customer data, which formed part of a data migration process that took place in 2019. • The Private Lounge platform was rebuilt in 2019. As part of this rebuild, the Organization migrated data sets of approx. 99,000 individuals from one server located in Germany to another server also located in Germany. • During this migration process, an unknown criminal appears to have gained access to the relevant data sets. • The current Private Lounge is not affected.
Affected individuals	The incident affected 99,233 individuals, including 599 Canadians, some of which are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Informed individuals to be vigilant in particular regarding phishing attempts and if they had uses the same password multiple times. • Sought to adopt improvements in its control environment for future IT migration projects and the operation of the Private Lounge platform as necessary. • Reported the breach to the German Data Protection authorities of the Federal State of Baden-Wuerttemberg and the State Criminal Policy office of Baden-Wuerttemberg. • Notified data protection authorities in relevant countries with data breach obligations.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 7, 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, *As the data is being offered for sale on the internet and includes potential username and password information we might expect data subjects to be targeted with phishing emails. While the passwords are hashed and salted, it is possible that they may be reconstructed and thus attempts to log in to user accounts on other sites where the data subject may have used similar passwords might be possible. Access to the AMG Private Lounge will not be possible using this login information, as the version of the AMG Private Lounge linked to this breach is no longer in use and was rebuilt in 2019 including a new login and updated password rules.*

	In my view, a reasonable person would consider that contact information, and particularly email addresses, in association with the individual's relationship to the Organization, could be used for phishing purposes. This increases the affected individuals' vulnerability to identity theft and fraud. Confirmed credentials could be used to compromise other online accounts. 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 reported, *As the AMG Private Lounge linked to the breach is no longer in use, the likelihood of harm is limited. However, while at least several years old, the use of the contact information for phishing emails seems possible*. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. The attacks appear to have been ongoing for an unknown period before the Organization discovered the threat.

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 contact information, and particularly email addresses, in association with the individual's relationship to the Organization, could be used for phishing purposes. This increases the affected individuals' vulnerability to identity theft and fraud. Confirmed credentials could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. The attacks appear to have been ongoing for an unknown period before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose 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 on July 7, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance