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	Porsche Centre Calgary (Organization)
Decision number (file number)	P2022-ND-62 (File #025392)
Date notice received by OIPC	April 1, 2022
Date Organization last provided information	May 19, 2022
Date of decision	November 2, 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 located in Calgary, Alberta, and 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, • date of birth, • email address, • mailing address, • telephone number, • email preferences, and • information about vehicle purchases. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• A database containing customer personal information was used without authorization by a former employee whose employment was terminated in 2021. • The unauthorized access was discovered on or about March 25, 2022, after customers notified the Organization about unsolicited emails received at email addresses "that they have only shared with the dealership." Some of the affected individuals explained "they had not given consent … to the sender or his organisation" and "have not signed up for the newsletter / information pdf" they received. • It is believed that the former employee retained a copy of the Organization's customer database - which they had access to during their employment - and are "utilizing the customer data base [sic] information to solicit and send spam that was not agreed to by … customers." It is also reported that "the individual in question has already tried to represent himself as a member of the company while accessing customer data." • The Organization's attempts to contact the unauthorized party and retrieve or destroy the records have been unsuccessful.
Affected individuals	The incident affected approximately 10,000 individuals.
Steps taken to reduce risk of harm to individuals	• Reported the incident to fightspam.gc.ca. • Continuing attempts to contact the former employee and retrieve or destroy the records. • Restricted access to customer data for existing users. • Requiring employees to "sign a document barring them from using procured company data after they are let go."
Steps taken to notify individuals of the incident	Affected individuals were not notified of the incident.
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 possible harms of "Spam, solicitation, and unauthorized use of information, breach of CASL Laws … [and] Information can be sent and shared online doxing customers." It is also reported that the unsolicited emails appear "very similar to information [the Organization] would routinely send to clients and is deceptive to the recipient." In a May 2022 update, the Organization reported "Identity theft would be an area of concern as the individual in question has already tried to represent himself as a member of the company while accessing customer data to do that."

	In my view, a reasonable person would consider that contact and identity information (name, email address, mailing address, telephone number, date of birth) and knowledge about individuals' relationship with the dealership could be used for the purposes of phishing, increasing the affected individuals' vulnerability to fraud and possibly identity theft. 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: *We do not believe there is any malicious intent, but we cannot confirm anything as we are not sure how far that breech [sic] as gone as this individual has had access to the entire database.* *… the individual in question has already tried to represent himself as a member of the company… [and] At this time, any copy of the data base or information that the individual had access to is still in possession by the individual.* In my view, the likelihood of harm resulting from this incident may be reduced due to the relatively low sensitivity of the personal information involved; receiving "spam" is not a significant harm. However, the likelihood of harm resulting from this incident may be increased because the personal information is being deliberately used without authorization and an attempt has been made to impersonate the Organization by an unauthorized actor whose motives are not known. Further, attempts to contact the unauthorized actor and retrieve or destroy the records have been unsuccessful; the personal information has been in the custody of the unauthorized actor since the termination of their employment in 2021.

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.

Contact and identity information (name, email address, mailing address, telephone number, date of birth) and knowledge about individuals' relationship with the dealership could be used for the purposes of phishing, increasing the affected individuals' vulnerability to fraud and possibly identity theft. These are significant harms.

The likelihood of harm resulting from this incident may be reduced due to the relatively low sensitivity of the personal information involved; receiving "spam" is not a significant harm.

However, the likelihood of harm resulting from this incident may be increased because the personal information is being deliberately used without authorization and an attempt has been made to

impersonate the Organization by an unauthorized actor whose motives are not known.

Further, attempts to contact the unauthorized actor and retrieve or destroy the records have been unsuccessful; the personal information has been in the custody of the unauthorized actor since the termination of their employment in 2021.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance