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	Don Wheaton Chevrolet GMC Buick Cadillac Ltd. (Organization)
Decision number (file number)	P2021-ND-006 (File #019030)
Date notice received by OIPC	January 19, 2021
Date Organization last provided information	January 20, 2021
Date of decision	February 16, 2021
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, • email address, • address, • telephone number, and • vehicle year/make/model/VIN/odometer reading/license plate number; MVA date; vehicle repair details and cost; photograph of vehicle; insurer, date of loss, claim #. 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. The Organization reported that some email addresses of the affected individuals in Alberta were business email addresses. As such, some of the information may qualify as "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(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "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 disclosure of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On December 23, 2020, the Organization's service desk received and opened an email that activated malware. • A single computer and single email address were infected. • On December 28, 2020, unusual activity in the email account led to it an investigation by IT and cyber security personnel. • The virus was discovered and removed immediately. The effect of the virus was not apparent at that time. • On January 5, 2021, a customer (insurance company) reported receiving two emails that had spoofed the Organization's email address; both had been blocked and quarantined by security software. • The Organization reported that it is likely that the contents of the affected email account were exfiltrated. • To date, one commercial customer and one individual customer reported emails spoofing the Organization's email account; all were blocked and quarantined by security software.
Affected individuals	The incident affected 4,000 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Notified individuals with email addresses that are suspected of having been exfiltrated. • Reminded recipients to use caution before opening emails that appear to have been sent by the Organization. • Activated stronger protection against cyber attacks. • Instituting training in cyber security for employees using company computers.

Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 13, 2021. The notification went to all email addresses that may have been affected including other companies' email addresses. The wording of the notification was broad to meet this situation.
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 that may occur as a result of the breach are: *a) identity fraud* *b) Individuals may receive malware via emails spoofing the body shop that, if not blocked by anti-virus software, could install a virus on their computers.* In my view, a reasonable person would consider that contact information such as name and email addresses, particularly in conjunction with transactional information, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 the likelihood of harm as: *a) Low. Because of its nature and low sensitivity, it is unlikely that the personal information involved would be used to commit identity fraud or other harm.* *b) Low. it [sic] is likely that most anti-virus software would block or quarantine spoofed emails containing malware.* In my view, a reasonable person would consider that 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 (phishing). Further, it appears the email account was exposed for approximately two (2) weeks.
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 such as name and email addresses, particularly in conjunction with transactional information, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 (phishing). Further, it appears the email account was exposed for approximately two (2) weeks.	

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 on January 13, 2020; however, the notification was not in accordance with the Regulation. **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 in writing, 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.**

Jill Clayton
Information and Privacy Commissioner