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	Herbers Autobody Repair Inc. (Organization)
Decision number (file number)	P2021-ND-028 (File #019005)
Date notice received by OIPC	January 15, 2021
Date Organization last provided information	January 21, 2021
Date of decision	February 23, 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 operates in 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, • email address, and • general information such as vehicle make and model. 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 December 30, 2020, the Organization was the victim of a phishing attack when a staff member opened an email attachment that contained malware.

	• The breach was discovered on January 4, 2021 when unusual emails were detected by the Organization's email filtering system. • The Organization investigated and found that the perpetrators could have gained access to personal information.
Affected individuals	The incident affected 3,390 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Contained the virus. • Contracting a third party to reviewing its security policies. • Holding internal refresher training with stakeholders to remind them about spam emails.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 7, January 15, 2021, January 20, 2021 and January 21, 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 "It would be an exposure of name (if it was in the outlook contacts) and email address, purchase order #'s and job numbers." In my view, a reasonable person would consider that email addresses, particularly in conjunction with name and relationship with the Organization, 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, *This malware was limited and contained in one computer. We feel confident that the harm will be minimal, as all they got was email addessses [sic], names, and some general information.* 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 seven (7) days.
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 email addresses, particularly in conjunction with name and relationship with the Organization, 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 seven (7) days.

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 7, January 15, 2021, January 20, 2021 and January 21, 2021 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner