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	The Driving Force Inc. (Organization)
Decision number (file number)	P2020-ND-010 (File #013735)
Date notice received by OIPC	October 11, 2019
Date Organization last provided information	October 11, 2019
Date of decision	February 12, 2020
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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • name, • employer/ company, • email address, • home and work telephone number, • address, • image of credit application and information contained in it, including social insurance number, • image of driver's license and information contained on it, • credit card information, • bank account information, • image of identification page of passport and information contained on it. 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 September 3, 2019, the Organization discovered that, due to a phishing scheme, an unauthorized third party gained access to the Outlook mailbox of one of its vehicle rental agents working out of Kelowna, British Columbia. • The Organization has not been able to determine the identity of the third party or whether any specific information within the account was actually accessed or downloaded. • The breach was discovered by the Organization's IT department on September 3, 2019.
Affected individuals	The incident affected 53 individuals, including 3 located in Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated a password reset, and completed a refresher course on phishing with the vehicle rental agent in question. • Implemented two-factor authentication for the account. • Researching additional measures to include technical security. • Offered 1 year free credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on October 11, 2019.
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 most likely types of harm that may result from the breach are fraud and identity theft". In my view, a reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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: *While the Company is not yet aware of any attempts to utilize the information, given: (a) the sensitive nature of information; (b) that there is evidence of malicious intent or purpose (the act was deliberate); (c) our assessment that the information may be used for fraud or identity theft; and (d) the number of individuals affected; there is a likelihood that harm could result.*

	I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The lack of reported misuse of the information to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even years after a breach.

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, identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The lack of reported misuse of the information to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even years after a breach.

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 individuals were notified in writing on October 11, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner