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., TDF Group Inc., Driving Force Investments Inc., 4505 Nunavut limited, Klondike Motors Inc., DF Western Inc., and The Driving Force Ltd. (collectively the "Organization")
Decision number (file number)	P2018-ND-058 (File #008017)
Date notice received by OIPC	March 14, 2018
Date Organization last provided information	March 14, 2018
Date of decision	May 8, 2018
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that all personal information involved in the breach is in electronic form, as email messages or attachments to email messages. It has identified several categories of information involved, as follows: <u>Category One</u> • The names, positions, and associated business contact information (primarily consisting of email addresses) of Organization employees. <u>Category Two</u> • The names and associated 2017 bonus compensation amounts for certain employees; • Payroll Earning History Report for certain employees, containing information such as name, earning description (minimum wage, etc.), employee number, employment status, pay date, cheque date, and amounts; • Name and associated position, hire date, base salary, pay class, and pay type of certain employees;

	• Names and associated overtime hours/compensation for the months March 2017 through January 2018, of certain employees; • Names and associated position and compensation amounts for 2016 and up to October 2017 of certain employees; • Names and associated month and day of working anniversary (year not specified) of certain employees; • Names and associated number of shares and dividends payable for 2017, of certain management and executive level employee shareholders of the Organization; • Names of employees considered for or invited to participate in the Organization's shareholder initiative; • Terms of Employment document for one management-level Organization employee, containing information such as name, position, and compensation. <u>Category Three:</u> • The personal mailing/home address of two employees; • Application and documents for work permit pertaining to one executive-level employee, containing information such as name, birthdate, intended position, job description, academic and work history, work history, and compensation; • Payroll documentation of one executive-level employee, including copies of two pages of the individual's passport, work permit, SIN confirmation, and bank account information for payroll deposit; and • C.V. of two executive-level employees of the Organization's parent organization, which contain information such as name, birthdate, and academic and work history. The Organization also reported that certain individuals belong to more than one category stated above. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On February 12, 2018, the Organization discovered an unauthorized forwarding rule attached to the Outlook mailbox of its President, such that incoming email messages to the mailbox were also being forwarded to an unauthorized third-party Gmail account.

	• Based on the data and information currently available, the unauthorized forwarding rule had been in place since at least November 15, 2017. • The Organization has ruled out malware, and believes the incident may be the result of a phishing scheme.
Affected individuals	The Organization has identified a total of 564 unique individuals in Canada affected by this incident.
Steps taken to reduce risk of harm to individuals	• Working with its service provider to determine the duration and impact of the incident. • Removed the unauthorized forward rule from the affected account, initiated a password reset, performed scans on the affected computer to confirm that no malware existed, and performed a factory reset on the President's mobile telephone. • Implemented two factor authentication for the affected account, as well as for the accounts of several other key executives and staff members. • On an organization-wide basis, ran a script to check all Outlook mailboxes to confirm no other forwarding rules in place, and disabled the ability for non-administrator accounts to set automatic forwarding rules in their mailboxes. • Researching additional measures to enhance security and authentication. • Notified the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia, as well as law enforcement.
Steps taken to notify individuals of the incident	The Organization sent an email/internal message to current employees on March 12, 2018, and a separate message on the same date to current employees in Category Two (with the exception of management, executive and shareholder employees). The Organization is in the process of notifying former employees, as well as independently notifying management, executive, and shareholder employees, and individuals in Category Three.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 that: *The information in Category One is the least sensitive, as this type of business information is not secret and generally well known to many third parties. However…we still consider this information to be of a sensitive nature.* *The information in Category Two is more sensitive, as this type of information of specific to the individuals involved and not well known to other parties… this information may be used as a start to an individual profile, for the purposes of fraud or identity theft. However, this information in and of itself will unlikely be sufficient to complete such profiles.*

	The information in Category Three is the most sensitive, as the type of information is more specific and may be used to complete an individual profile for the purposes of fraud or identity theft. The Organization also said that "The harm is significant. The information in Category One may be utilized for phishing purposes, and the information in Category Two and Category Three may be used the purposes of fraud and identity theft." I agree with the Organization's assessment. The comprehensive contact, identity and employment information at issue could be used to cause the significant harms of identity theft, fraud and phishing.
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) the length of time for which the unauthorized forwarding rule was in place; (e) that there is evidence of malicious intent or purpose (the act was deliberate); (d) our assessment that the information may be used for fraud or identity theft, and (e) the number of individuals affected; there is a likelihood that harm could result." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action and misdirection of email), the information may have been exposed for approximately 3 months, and a relatively large number of individuals were affected.

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 as a result of this incident.

The comprehensive contact, identity and employment information at issue could be used to cause the significant harms of identity theft, fraud and phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action and misdirection of email), the information may have been exposed for approximately 3 months, and a relatively large number of individuals were affected.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization began notifying affected individuals by email on March 12, 2018 and further notification was in progress at the time the Organization reported this incident to my office. **I require the Organization to confirm to my office that all affected individuals in Alberta have been notified, in compliance with the Regulation, within 10 days of the date of this decision.**

Jill Clayton
Information and Privacy Commissioner