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	FGL Sports Ltd., a wholly owned subsidiary of Canadian Tire Corporation Limited (Organization)
Decision number (file number)	P2016-ND-58 (File #000836)
Date notice received by OIPC	May 15, 2015
Date Organization last provided information	June 3, 2016
Date of decision	September 1, 2016
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"	I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • date of birth, • salary information, • employee identification number, • business email address, • human resource job code, • organization unit code, • current position start date, • hire date, • gender, • manager's identification number, • pro-ration of merit increase, • department, • enrollment plan, • annual work hours, • alternative earnings, • old salary, and • performance rating.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• A laptop computer containing the information at issue was stolen from an employee's vehicle on May 2, 2015. • The laptop was password-protected, but neither the file containing personal information nor the laptop was encrypted.
Affected individuals	A total of 1,025 employees located in corporate offices in Calgary, Laval, Mississauga and Markham were affected. Of these, 672 individuals are from Alberta.
Steps taken to reduce risk of harm to individuals	• The laptop computer required password authentication prior to authorizing access to information stored in it. • An investigation into the incident was conducted. • The matter was reported to law enforcement. • Free identity theft protection was provided to affected employees for one year. • The Organization reported that considerations have been made to provide appropriate training to employees who deal with personal information and to implement encryption. • The employee who was involved in the incident was warned for a breach of the Organization's policy.
Steps taken to notify individuals of the incident	Affected employees were notified of the incident by letter emailed on May 11, 2015.
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 incident "posed a potential - though possibly remote concern for identity theft" and also that "The personal information in the File that would be most susceptible to a risk of identity theft is name and birthdate. The remainder or the information, while sensitive, would not likely lead to identity theft." In my view, the identity and employment information at issue could be used to cause the harms of identity theft and fraud, and possibly hurt, humiliation and embarrassment (salary or performance information). Email addresses could be used for phishing purposes. 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 that it does not believe affected individuals are at real risk of significant harm because: • "The incident does not involve nefarious activity targeted specifically at the laptop. The laptop was in a bag and not visible prior to the entry to the locked vehicle through the window. We have no reason to believe the perpetrator(s) had knowledge that the laptop was inside the bag or that the laptop contained the File. • There have been no reports of identity theft from any affected individuals at present." In my view, there is a real risk of harm resulting from this incident. The incident is the result of malicious intent (theft), the laptop was not encrypted, and has not been recovered. While the Organization believes the information at issue was not the target of the theft, this cannot be known for sure. I do not believe that the lack of reported incidents of identity theft to date is a factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data 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.

The identity and employment information at issue could be used to cause the harms of identity theft and fraud, and possibly hurt, humiliation and embarrassment (salary or performance information). Email addresses could be used for phishing purposes. These are significant harms. The incident is the result of malicious intent (theft), the laptop was not encrypted, and has not been recovered. While the Organization believes the information at issue was not the target of the theft, this cannot be known for sure. I do not believe that the lack of reported incidents of identity theft to date is a factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

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

I understand the Organization notified the affected individuals by letter emailed on May 11, 2015 in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner