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	Tween Brands Canada Stores Ltd., operating under the Justice brand (Organization)
Decision number (file number)	P2017-ND-160 (File #007100)
Date notice received by OIPC	November 15, 2017
Date Organization last provided information	November 15, 2017
Date of decision	November 30, 2017
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 affected individuals 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 may have involved the following information: • name, • driver's license number. 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	• On September 7, 2017, the Organization discovered signs indicating attempts were made to gain access to one of their web servers.

	• The incident was discovered after the Organization's database administration team discovered a high number of failed SQL login attempts. The Organization's IT Security team investigated these reports and identified signs of unauthorized access to a database server. • Findings from the investigation determined that an unauthorized individual may have gained access to the server and then used that access to connect to a database server. The database included information regarding certain tax exempt transactions, which included the name and driver's license number of three Alberta residents. • The Organization reported the earliest evidence of unauthorized access was September 5, 2017 until the incident was discovered September 7, 2017.
Affected individuals	The incident affected three (3) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately removed the server, launched an investigation and engaged third-party experts to assist in the investigation. • Worked closely with the third-party security experts to develop enhanced security measures and prevent similar occurrences. The enhanced security measures include endpoint protection software and reduced access rights to sensitive data based on least privilege. • Arranged to offer potentially affected individuals 12 months of identity repair, identity theft monitoring, and credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals in Alberta were notified in writing on November 15, 2017.
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 loss of a driver's license number may result in potential harms, such as financial loss, fraud, identity theft, and potential negative effects on a credit record." I agree with the Organization. The identity information at issue could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit record. 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 it "…has no indication that any personal information was used in any way as a result of this incident, and the risk of further exposure to personal information has been contained." In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion). Although the Organization is not aware of the personal information being used to cause harm at this time, and steps have been taken to detect credit card fraud, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud occurring in the future.

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 information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit record. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion). Although the Organization is not aware of the personal information being used to cause harm at this time, and steps have been taken to detect credit card fraud, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud occurring in the future.

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

I understand the Organization notified the affected individuals in writing on November 15, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner