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	Don Best Sports Corporation and DBS Canada Corporation (together, "Don Best"), a subsidiary of Scientific Games Corporation (the Organization) The Organization acquired Don Best on November 1, 2018
Decision number (file number)	P2019-ND-081 (File #010716)
Date notice received by OIPC	January 11, 2019
Date Organization last provided information	February 15, 2019
Date of decision	June 24, 2019
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 is a Nevada-based company that operates in the gaming and lottery industries, 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, • address, • telephone number, • username (the customer's email address), and • password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected when individuals made purchases on the Don Best website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 21, 2018, during the course of conducting a cyber risk assessment of the Don Best network infrastructure prior to integrating that environment into the Organization's network, the Organization discovered that, between October 12, 2018 and October 28, 2018, Don Best had been the subject of a malware attack that resulted in an unauthorized individual gaining access to a Don Best customer database. • While the unauthorized user was able to view data, based on a forensic examination of the Don Best servers, the unauthorized user acquired usernames (e-mail addresses) and passwords to the accounts.
Affected individuals	The incident affected 137 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Blocked the unauthorized user's IP address. • Migrated the databases with vulnerability to more current and supported SQL versions on a server with a more current operating system. • Removed the malware in the migration process. • Placed intrusion detection monitoring systems on the migrated data. • Resetting all customers' passwords. • Notified all affected individuals. • Informed affected individuals on how to protect their personal information and how to request a fraud alert on their credit file.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 6, 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated "Be alert to any requests for personal information, in particular financial institutions, account numbers and passwords… and remain vigilant by reviewing your financial accounts statements and credit reports for signs of fraud." In my view, a reasonable person would consider that the contact information and credentials (email username, password) could be used for phishing and to compromise other online accounts, 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 did not specifically assess the likelihood that significant harm would result from this incident. 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 (deliberate intrusion). Further, the information appears to have been exposed for over two weeks.

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 information and credentials (email username, password) could be used for phishing and to compromise other online accounts, 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 (deliberate intrusion). Further, the information appears to have been exposed for over two weeks.

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 in a letter dated February 6, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner