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	BPS Diamond Sports Corporation (Organization)
Decision number (file number)	P2013-ND-52 (File #P2550)
Date notice received by OIPC	January 13, 2014
Date Organization last provided information	March 5, 2014
Date of decision	May 20, 2014
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"	Organization is federally incorporated. 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"	Credit card numbers, expiry dates and the Card Verification Value (CVV) codes for the credit cards were involved in this incident. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	Between November 6 and November 8, 2013 an unauthorised third party gained access to certain computer systems located on a server. The access to the systems was gained through hacking. The purpose of the hack is unknown.

	The server was an asset from a company purchased by the Organization. It was located outside of the Organization's secure environment, hosted by a third party service provider. Computer systems on the old server included an accounting program which contained unencrypted credit card information. The Organization is unable to determine if the credit cards were for personal use or corporate cards issued for company use.
Affected individuals	165 affected individuals in Canada; 12 affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	The information contained on the affected server was migrated to a new more secure environment.
Steps taken to notify individuals of the incident	Notification sent by mail to affected individuals on January 13, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized the affected individuals may be at risk for identity theft, fraud and financial loss. As well, their credit record could be negatively impacted. In my view, the personal information involved is highly sensitive. It includes all of the information designed to act as security features for a credit card. I agree that this information could be used to cause the harms of fraud, financial loss and/or identity theft and could have a negative impact on an affected individual's 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 that, due to the sensitivity of the personal information involved, it considered there to be a real risk of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed through a successful hacking attempt by an unknown third party and has not been recovered.
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 personal information involves sensitive financial information. The information has been accessed by a successful hacking attempt and has not been recovered. These factors contributed significantly to my decision.	

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 that this has already been completed by the Organization.

Jill Clayton
Information and Privacy Commissioner