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	Activision Blizzard, Inc. (Organization)
Decision number (file number)	P2017-ND-107 (File #006112)
Date notice received by OIPC	July 24, 2017
Date Organization last provided information	July 24, 2017
Date of decision	August 3, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify those individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an American video game publisher and 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, • payment card number, expiry date, and possibly security code. The following information may also be at issue: • name, • email address, • telephone number, • address, and • other information. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information is associated with a payment card used to book hotel reservations through a central reservations system.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization was notified that an unauthorized party obtained access to information associated with payment cards used to book hotel reservations through a central hotel reservation system (CRS) subcontracted by the Organization's travel partner, American Express. • The Organization understands from the subcontracted service provider that the attacker obtained access to account credentials that permitted access to a subset of hotel reservations processed through the CRS. • The unauthorized access took place between August 10, 2016 and March 9, 2017.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• The service provider engaged a cybersecurity firm to support its investigation, and notified law enforcement and payment card brands about the incident. • The Organization will notify its employees, contractors, and other related individuals about the incident and recommend that they remain vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring free credit reports for any unauthorized activity. • Expects to notify at least one attorney general's office in the U.S.
Steps taken to notify individuals of the incident	The Organization reported it would notify the affected individual in Alberta by email on July 21, 2017, and provided a copy of the notification statement.
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 "It is possible that some fraudulent transactions may be carried out with the cards impacted by this incident." In my view, the contact, financial and profile information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. These are all 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 "…we do not believe the likelihood of harm is great. Major credit card companies monitor for fraud as well as have rules that restrict them from requiring individuals to pay for fraudulent charges that are timely reported [sic]. In our notification to impacted individuals, we will recommend that they remain vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring free credit reports for any unauthorized activity." In my view, the likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost seven (7) months.

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 individual.

The contact, financial and profile information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. These are significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate intrusion) and the personal information was exposed for almost seven (7) months.

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

I understand the Organization notified the affected individual in Alberta by email on July 21, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner