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	Take-Two Interactive Software, Inc. (Organization)
Decision number (file number)	P2021-ND-262 (File #021162)
Date notice received by OIPC	May 15, 2021
Date Organization last provided information	November 19, 2021
Date of decision	February 8, 2022
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 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: • email address, • order history including date and value of purchase, and • valid credentials. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On April 6, 2021, the Organization discovered that its web-store was the subject of a credential stuffing attack which took place between March 19 and 30, 2021. • The unauthorized third party logged into accounts using valid credentials obtained from an unknown source. • Once logged in, the unauthorized third party redeemed game codes and had access to personal information in the accounts.
Affected individuals	The incident affected 11 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Took the web-store offline to prevent further compromise. • Investigated the incident. • Deactivated some account functionality that was abused during the attack. • Revoked stolen game codes. • Implemented measures to monitor for unusual account activity. • Implemented dark web monitoring. • Blacklisted malicious IP addresses. • Forced password changes for all web-store accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about May 6, 2021.
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 provide an assessment of possible harms that could be caused to affected individuals as a result of the incident. However, it forced a password reset and recommended affected individuals change passwords for other online accounts using the same credentials. In my view, a reasonable person would consider that the email addresses and knowledge that the affected individual had a valid account could be used for the purposes of phishing or spear-phishing, introducing the possible harm of fraud. Known valid credentials could be used to compromise other online accounts. 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 "believes that there is a low risk of actual harm to impacted individuals as a result of the incident" and that "there was no evidence of misuse of personal information." 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 malicious intent (deliberate intrusion). The lack of reported misuse of the personal information does not mitigate against future harms as fraud and phishing can occur months or years after a 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.

A reasonable person would consider that the email addresses and knowledge that the affected individual had a valid account could be used for the purposes of phishing or spear-phishing, introducing the possible harm of fraud. Known valid credentials could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate intrusion). The lack of reported misuse of the personal information does not mitigate against future harms as fraud and phishing can occur months or years after a breach.

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 by letter on or about May 6, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner