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	Big Fish Games (Organization)
Decision number (file number)	P2016-ND-56 (File #000312)
Date notice received by OIPC	February 19, 2015
Date Organization last provided information	February 23, 2015
Date of decision	August 30, 2016
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"	The Organization is 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, • address, • credit card number, expiry date and security code (CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 12, 2015, through a routine review of logs, the Organization discovered that an unknown individual(s) installed malware on the Organization's online purchasing system. • The malware appears to have intercepted payment details of customers who made payments via the online system. • The incident affected customers who made purchases between December 24, 2014 and January 8, 2015.

Affected individuals	There were 362 affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the Federal Bureau of Investigation. • The malware was removed and a security forensics firm was retained to assist in the investigation of the incident. • Payment card networks were notified and affected individuals were advised to monitor their accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent February 11, 2015.
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 that the information at issue could be used to "make fraudulent charges". I agree that the personal information involved could be used to make fraudulent charges, as well as generally cause the harms of 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 reported that it believes "the likelihood of significant harm is low." I understand the Organization says this because "consumers are typically not responsible for unauthorized charges made under these circumstances." In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for over 2 weeks before the Organization became aware of the breach. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.
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 involved could be used to make fraudulent charges, as well as generally cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for over 2 weeks before the Organization became aware of the breach. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.	

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 the Organization notified affected individuals in accordance with the Regulation by letter sent February 11, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner