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	Product Madness, Inc. (Organization)
Decision number (file number)	P2018-ND-092 (File #009327)
Date notice received by OIPC	June 18, 2018
Date Organization last provided information	June 18, 2018
Date of decision	August 1, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved stolen laptops that could have contained the following information about certain of the Organization's users: • full name, • email address, • total amounts spent on in-game purchases, • last payment date, • information relating to the use of the game (such as last visit date and game credit balance), • mailing address, telephone number and date of birth if users voluntarily submitted such information. The Organization reported that not all of this data was stored for all customers. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On Tuesday, May 15, 2018, the Organization's San Francisco, California office was broken into and certain property was stolen, including fourteen (14) company laptops. • The Organization believes that certain personal information was stored on the stolen devices. The Organization does not have any evidence that the information on the stolen laptops has been accessed or used. • The Organization reports that "Based on the findings of the investigation to date, the theft appears to be motivated by a desire to steal physical property, and not to acquire personal information."
Affected individuals	The Organization reported there are approximately 99 potentially-impacted users residing in Canada, but does not know for certain how many of these users reside in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement and assisting in the criminal investigation into the theft. • Reset the passwords on all stolen laptops and enhanced physical security measures. • Providing a dedicated telephone number and email address for individuals to use to ask further questions about the incident. • Providing affected individuals with access to identity theft protection services for a period of 12 months at no cost. • Recommending that users remain vigilant opening emails, especially emails seeking personal information.
Steps taken to notify individuals of the incident	The Organization reported that it is notifying two categories of potentially-affected individuals: (i) individuals whose customer record included name or email address and date of birth; and (ii) individuals whose customer record included name or email address and whose in-game purchases exceeded US $50,000 over their lifetime of play. The Organization also said that it is using an in-game chat function to attempt to notify those users for whom the Organization does not have a valid email address (including where the notification email bounced back).
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 the harm(s) might result from this incident, but its letter notifying affected individuals said "We also recommend that you remain vigilant of the risk of identity theft and phishing sites or emails, which seem to mimic legitimate sites or senders and that may sometimes reference information about you to trick you into providing more of your personal information." In my view, the contact (including email address), profile (game and payment history) and identity information at issue could be used to cause the significant harms of identity theft and fraud, and phishing.

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 "… does not believe there is a real risk of harm to individuals due to the fact that the theft appears to have been motivated by a desire to steal the stolen property, and not to acquire personal information. Additionally, [the Organization] has conducted monitoring since the incident and has not seen any indications that personal information stored on the stolen laptop actually has been accessed or used." In my view, there is a real risk of harm resulting from this incident. The breach was the result of malicious intent (deliberate break-in and theft of laptops), the Organization did not report recovering the laptops nor any information as to why it believes the theft was motivated by a desire to steal property and not information. The fact that there have been no indications or reports about access and use of information stored on the laptops does not mitigate potential harm, as unauthorized access and use could still occur at any time in the future.

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 as a result of this incident.

The contact (including email address), profile (game and payment history) and identity information at issue could be used to cause the significant harms of identity theft and fraud, and phishing. The breach was the result of malicious intent (deliberate break-in and theft of laptops), the Organization did not report recovering the laptops nor any information as to why it believes the theft was motivated by a desire to steal property and not information. The fact that there have been no indications or reports about access and use of information stored on the laptops does not mitigate potential harm, as unauthorized access and use could still occur at any time in the future.

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

The Organization reported that it will be notifying affected individuals. **I require the Organization to confirm to my office within 10 days of the date of this decision that affected individuals in Alberta were notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner