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	Zynga Game Ireland Limited (Organization)
Decision number (file number)	P2019-ND-181 (File #013343)
Date notice received by OIPC	September 30, 2019
Date Organization last provided information	October 22, 2019
Date of decision	December 4, 2019
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 incorporated in the Republic of Ireland and maintains a website which provides online and mobile gaming and social networking sites to users. 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: • name, • username, • password, • email address, • telephone number, • photograph, • social media ID, • date of birth, and • location. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 2, 2019, the Organization discovered that certain player account information may have been illegally accessed by outside hackers on or about August 31, 2019. • The games, group of games, and data sources affected were: Draw Something (formerly OMGPOP); Poker; Games with Friends; and one additional table that is not tied to a particular game. • The Organization does not believe that any financial information was accessed.
Affected individuals	The incident affected 73,000 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated with assistance of consultants and third party-forensic firm. • Eliminated access to affected network resources. • Protected accounts from invalid logins e.g. where passwords may have been accessed. • Posted a blog notifying the public regarding the issue. • Contacted law enforcement and regulatory authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email the week of September 30, 2019, and on October 23, 2019.
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 specifically identify any harm that might result from this incident, but its "Player Security Announcement" to users said "if you used your [Organization] password on another website or app, it is good practice to change your password on the other website or app." In my view, a reasonable person would consider that the contact and identity information (date of birth, photograph, and social media ID) at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. 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	The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the

cause and effect relationship between the incident and the possible harm.	personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately 3 days.

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 contact and identity information (date of birth, photograph, and social media ID) at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials could be used to compromise other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately 3 days.

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 email the week of September 30, 2019, and on October 23, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner