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	Electronic Arts, Inc. (Organization)
Decision number (file number)	P2022-ND-053 (File #026988)
Date notice received by OIPC	August 15, 2022
Date Organization last provided information	August 15, 2022
Date of decision	August 30, 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 the 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 some or all of the following information: • name, • email address • username, • job role, physical location (office address or reference to country), • work telephone number, • membership of email distribution list, and • employee led groups supporting certain causes. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported*, "Affected data subjects were employees, non-employee workers, and business partners (in the latter case, only in relation to name and email address for the large majority of data subjects concerned)."* As such, some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business

	telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to the personal information about the 326 individuals in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 1, 2022, an internal active directory contact list with details of the Organization's workers and business partners was posted on an underground hacking community channel within the messaging platform, Telegram. • The information was then reposted on August 4, 2022, on a different channel on the Telegram platform. • The Organization learned of these postings on August 11, 2022. • The attacker obtained access to the credentials of a service account (i.e., an account provisioned for internal automated services, not an account belonging to a specific individual). • The Organization continues to investigate how the attacker gained access to this account. • The Organization reported it is currently unaware of any actual misuse of this information.
Affected individuals	The incident affected 23,598 individuals, including 326 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	Steps taken by the Organization includes, but are not limited to: • Mitigated risk by providing support to the affected individuals. • Issued a legal takedown to the platform requesting removal of the information.

	• Reset the credentials of the service account. Increased the number of conditional access control policies to prevent its use in this way again. • Taking equivalent actions with regard to other similar service accounts. • Performing an audit of all applications to ensure that they are correctly scoped. • Performing penetration tests to identify any other architectural flaws and remediate those as appropriate.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 12, 2022.
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, *To the best of our knowledge, no detriment to individuals has arisen at this time. We identify a future risk in the potential for more sophisticated and pointed phishing attempts based on this information, which we will mitigated [sic] by promoting awareness.* In my view, a reasonable person would consider that the name and email address, along with the other information at issue, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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, *The information was posted on an underground hacking community channel where the participants suggested using the information for phishing attempts. We therefore assess the potential harm as credible.* I agree with the Organization's assessment. A reasonable person would consider 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 and posting on an underground hacking community channel). The Organization reported, "*To the best of our knowledge, no detriment to individuals has arisen at this time*." In my view, the lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data 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.

The name and email address, along with the other information at issue, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 and posting on an underground hacking community channel). The Organization reported, "*To the best of our knowledge, no detriment to individuals has arisen at this time*." In my view, the lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

I require the Organization to notify the affected individuals whose 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 on August 12, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner