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	News America Marketing Digital LLC (Organization)
Decision number (file number)	P2020-ND-027 (File #013684)
Date notice received by OIPC	August 30, 2019
Date Organization last provided information	August 30, 2019
Date of decision	March 4, 2020
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 individual 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 of affected individuals: • first and last name, • email address, • date of birth (optional), • location (i.e. province), • email preferences, • IP addresses from which the device accessed the service, • the last time accessed by each IP address and user agent, • security preferences, and • legal and privacy settings. The Organization reported that "…not all users would have all of the above-noted information available through their accounts". This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

	The Organization maintains "…that it is not subject to the jurisdiction of the Office of the Information & Privacy Commissioner of Alberta". In my view, given the Organization is an "organization" as defined in PIPA, and the information at issue qualifies as "personal information" as defined in PIPA, PIPA applies to the extent the information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization learned an unauthorized third party attempted to gain access to Checkout 51 accounts via the Checkout 51 login application programming interface (API) between July 6 - 12, 2019. • Based on the Organization's investigation, the incident did not arise from a breach of the Organization's security safeguards; rather, the breach was caused by the reuse of usernames and passwords by users that may have been obtained by previous third party hacking incidents.
Affected individuals	The incident affected 247 accounts globally, including one confirmed as registered to a member residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Previously notified members to update their passwords and required passwords for compromised accounts be changed. • Updated monitoring/alerting systems for intrusion detection. • Analyzed application logs and implemented additional controls to block traffic. • Forced a reset of the user password for the affected Alberta resident. • Notified the affected individual in Alberta. • Enhancing its safeguards by implementing a network protection tool.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by email on July 13, 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	The Organization reported: *In most …accounts, not every field of personal information listed would have been available in the context of this incident. For example, date of birth is an optional field that*

important, meaningful, and with non-trivial consequences or effects.	*is only collected if provided by a member when signing up for the Checkout 51 service.* *Although the unauthorized third party may have been able to access personal information in this instance, the actual information that was accessed is non-sensitive in nature and does not pose a real risk of significant harm to the affected individuals.* In my view, a reasonable person would consider that contact and identity information (i.e. date of birth) could be used for identity theft and fraud. As well, email addresses could be used for the purposes of phishing, increasing the affected individual's vulnerability to 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 "…there has been no evidence of misuse of the personal information in question. To confirm, no theft or loss of users' cash back credits occurred as a result of the unauthorized access." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed over the course of a week. The fact there are not reports of actual harm to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

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 contact and identity information (i.e. date of birth) could be used for identity theft and fraud. As well, email addresses could be used for the purposes of phishing, increasing the affected individual's vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed over the course of a week. The fact there are not reports of actual harm to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

I require the Organization to notify the affected individual 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 the affected individual in Alberta in an email dated July 13, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner