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)	P2021-ND-288 (File #010188)
Date notice received by OIPC	October 26, 2018
Date Organization last provided information	October 25, 2019
Date of decision	February 24, 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 reported that it "…owns and operates the "Checkout 51" service, which enables consumers to earn cash back credits by selecting product offers and purchasing the featured products." The Organization also said it "… is providing the information set out below on a courtesy basis, however, it is the company's respectful position that the relevant data flows are not subject to the jurisdiction of the Office of the Information & Privacy Commissioner of Alberta." In an October 25, 2019 email, the Organization clarified its position… *…that PIPA is not constitutionally operative in respect of the transborder data flows involved with the Checkout 51 platform.* *… While the Company maintains its legal position on the question of jurisdiction set out above, the Company's correspondence of October 26, 2018 was intended to effectively provide your Office with the same information that would be required under section 34.1, with a view to being as transparent as possible and ensuring your Office was aware of the incident. Hence assuming, though not*

	conceding, that your Office does have jurisdiction in transborder situations such as this one, you will have received de facto notification of the information required. In response to the Organization's position, I note that section 3 of PIPA says "The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations …". Section 4 says "Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information." [my emphasis] The Organization is an "organization" as defined in section 1(1)(i) of PIPA. PIPA does not contain any territorial or constitutional limitation. I am aware that the *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219 (the Exemption Order) states: *An organization, other than a federal work, undertaking or business, to which the Personal Information Protection Act, S.A. 2003, c. P-6.5, of the Province of Alberta, applies is exempt from the application of Part 1 of the Personal Information Protection and Electronic Documents Act, in respect of the collection, use and disclosure of personal information that occurs within the Province of Alberta.* The Exemption Order sets out the territorial limitation of the Province of Alberta. With the exception of federal works, undertakings or businesses, organizations that collect, use and disclose personal information within Alberta are exempt from the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and PIPA applies. PIPEDA applies to the transborder flow of personal information. However, as provided by the Exemption Order, PIPEDA does not apply to the personal information collected, used or disclosed within Alberta. I do not lose jurisdiction over the collection, use or disclosure of personal information within Alberta just because the personal information subsequently enters a transborder flow. Such an interpretation would result in PIPEDA applying to the collection, use or disclosure of personal information within Alberta, when the Exemption Order says that PIPEDA does not apply. Finally, the Exemption Order is specific only as to the collection, use or disclosure of personal information within Alberta. Consequently, any collection, use or disclosure of personal

	information within Alberta brings an organization under my jurisdiction, regardless of where the organization may be located. Given the above, it is my view that, to the extent the personal information at issue in this matter was collected by the Organization in Alberta, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first and last name, • email address, • date of birth, • location (i.e. province), • IP address from device that accessed the service, • time of the last access of the services, and • user agent (e.g. the type of web browser and operating system) that last access the services. (Note: 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. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between September 27 and October 4, 2018, an unauthorized third party attempted to gain access to Checkout 51 accounts via the Checkout 51 login application program interface (API). • The incident arose out of an apparent reuse of usernames and passwords. The third party may have attempted to gain access to the Checkout 51 accounts of users who use the same username and password on multiple websites. • When a new device or web browser successfully accesses a user's Checkout 51 account using the user's username and password, the Organization sends an email to let the user know account access has occurred. During the relevant period of time, 34,000 such login notifications were provided globally, including notifications sent to 758 Alberta residents. A number of users responded to the notifications indicating that they had not logged-in to their Checkout 51 account. None of these responses were from Alberta residents.

	• The Organization investigated and found the data that may have been accessed by unauthorized individuals consisted "solely of non-sensitive information available through each user's Checkout 51 account". Of the 34,000 logins, 258 had a change in email address or mailing address. After reviewing these account changes, the Organization indicated that none appeared to be obviously suspicious in nature and none of these 258 account holders were residents of Alberta. • The Organization reported that there is no evidence that the affected personal information has been misused as a result of the incident and does not believe that the incident poses a real risk of significant harm.
Affected individuals	The Organization reported this was an incident "involving personal information of 758 Alberta residents", but also said it "…does not know whether some, all or none of the accounts of Alberta residents were actually accessed by an unauthorized individual."
Steps taken to reduce risk of harm to individuals	The Organization reported it "conducted an in-depth investigation into this matter, notified all individuals in Alberta who may have been affected by this incident, forced a reset of all user passwords and continues to monitor its systems through its 24/7 Information Security Program."
Steps taken to notify individuals of the incident	The affected individuals were notified by email dated October 26, 2018.
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 "Although the unauthorized third party may have been able to access personal information in this instance, the actual information that was accessed does not pose a real risk of significant harm to the affected individuals." However, the Organization's notice to affected individuals recommended "Using unique passwords for each account", "Monitoring your email for phishing scams", and "Review any suspicious login activity…". In my view, a reasonable person would consider that contact, identity and user account information, particularly in conjunction with email addresses and confirmed compromised credentials, could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' 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 it "…does not believe that the incident poses a real risk of significant harm to affected individuals" and noted that "there has been no evidence of misuse of the personal information in question" [emphasis in original]. 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 for approximately one month. The lack of reported misuse or incidents to date is not a mitigating factor, as phishing, identity theft and fraud can occur 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.

A reasonable person would consider that contact, identity and user account information, particularly in conjunction with email addresses and confirmed compromised credentials, could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing affected individuals' 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 for approximately one month. The lack of reported misuse or incidents to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

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 the affected individuals by email dated October 26, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner