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	Hudson's Bay Company (Organization)
Decision number (file number)	P2018-ND-152 (File #009844)
Date notice received by OIPC	September 25, 2018
Date Organization last provided information	September 25, 2018
Date of decision	November 23, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and 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: • first and last name, • mobile telephone number, • email address, and • postal code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 12,2018, the Organization's third party service provider, Vibes Media, LLC, reported that an unauthorized third party was able to gain access to the service provider's web application and obtain a copy of contact information of certain (but not all) customers of the Organization who were enrolling to receive marketing messages via text on their mobile devices.

	• The unauthorized third party obtained a copy of database records that contained the information at issue. • The Organization's service provider confirmed that it was able to identify and eliminate the vulnerability within the impacted web application on August 17, 2018. • The incident did not affect any of the Organization's systems or databases.
Affected individuals	The incident affected 2,066 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	• Worked with the service provider to address the issue. • The service provider confirmed that, upon learning about the incident, it promptly commenced a comprehensive investigation, contacted law enforcement and engaged outside cybersecurity professionals to assist in its investigative efforts. • The service provider confirmed that it has taken additional measures to further strengthen its cybersecurity program, including enhancing its security monitoring capabilities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email.
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 potential harms that might result from this incident. In my view, a reasonable person would consider that the contact and profile information (customer of the Organization), and email addresses and mobile telephone numbers in particular, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm.
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 did not specifically assess the likelihood of harm resulting from this incident, but reported that its service provider "…confirmed that it was not aware of any subsequent misuse of the contact information of [the Organization's] customers". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). It appears the information was exposed for at least five (5) days. The fact the service provider is not aware of misuse at this time does not mitigate potential harm.

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 profile information (customer of the Organization), and email addresses and mobile telephone numbers in particular, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm. The likelihood of harm is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). It appears the information was exposed for at least five (5) days. The fact the service provider is not aware of misuse at this time does not mitigate potential harm. 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. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner