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	Bath & Body Works Direct, Inc. (the Organization)
Decision number (file number)	P2020-ND-144 (File #014832)
Date notice received by OIPC	January 2, 2020
Date Organization last provided information	February 18, 2020
Date of decision	November 6, 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 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • email address, • mailing address (if entered), • birth day and month (not year), • telephone number, and • possibly last 4 digits of payment card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 2, 2019, the Organization learned that an unauthorized individual gained access to personal information in certain online accounts from approximately September 17, 2019 to November 23, 2019. • The Organization believes that the individual capitalized on a breach of another company's system where the customer may have used the same login information. • The Organization later reported that "…the unauthorized access also may have occurred until [the Organization] implemented additional safeguards on January 15, 2020."
Affected individuals	The incident affected 38 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to secure the accounts and determine the nature of the issue. • Coordinating with law enforcement authorities. • Disabled affected passwords and asking customers to make new ones. • Forced an additional reset of affected passwords and asking customers to make new ones.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on December 23, 2019 and again on February 18, 2020.
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 the potential harm(s) that might result from this incident, but its notification to affected individuals said "Please monitor your … account for suspicious activity" and "Promptly change the username and password on all other online accounts for which you use the same or similar username and password." In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing 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 did not provide its assessment of the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the risk of harm is increased as the incident appears to be the result of deliberate, malicious action. The information may have been exposed for almost four months.

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 the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The risk of harm is increased as the incident appears to be the result of deliberate, malicious action. The information may have been exposed for almost four months. 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 affected individuals were notified in writing on December 23, 2019 and again on February 18, 2020. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner