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	Blue Buffalo Company, Ltd. (Organization)
Decision number (file number)	P2021-ND-121 (File #017731)
Date notice received by OIPC	October 9, 2020
Date Organization last provided information	March 31, 2021
Date of decision	April 27, 2021
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 based in Wilton, Connecticut, USA, 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: • name, • username, • password, • email address, • mailing address, and • telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 31, 2020, an unauthorized party gained access to the Organization's network via the exploitation of a vulnerability present on one of the Organization's servers. • After the initial breach, the unauthorized party deployed malware and network penetration tools, extending the attack to other systems and user accounts on the Organization's network. • The breach was discovered on September 1, 2020 when the Organization's security team detected the attacker's activities.
Affected individuals	The incident affected 27 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Worked with a cybersecurity firm to block the unauthorized actor's access, secure the network, and investigate the incident. • Patched the exploited vulnerability and strengthened vulnerability management capabilities. • Forced a password reset for individuals who did not voluntarily change their network password after the date of the incident. • Encouraged individuals to change usernames and passwords for other online accounts that used the same or similar credential combinations.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 1 and 2, 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 reported: *We see the assessment of possible harms as low, considering there was no observed evidence of data exfiltration and given the limited and non-sensitive nature of the personal information that was impacted … given that email addresses were impacted, there is a potential risk of email phishing scams.* In my view, a reasonable person would consider the contact information at issue, in combination with email addresses, could be used for the purpose of phishing, increasing vulnerability to identity theft and fraud. Credentials may be used to compromise other online accounts. 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	The Organization reported: *[I]n our view, the risk is low due to no observed evidence of exfiltration and the limited and non-sensitive nature of the personal information impacted. We are not aware of any*

cause and effect relationship between the incident and the possible harm.	*information or complaints in respect of email phishing scams in connection with this incident.* *The investigation found no evidence within the in-scope systems and available network logs that supported a conclusion that data exfiltration occurred.* In my view, the likelihood of harm is increased because the personal information was compromised due to the malicious action (deliberate intrusion, deployment of malware and network penetration tools) of an unauthorized actor. Further, a lack of reported incidents does not mitigate against future harms, as phishing, identity theft, and fraud can happen months or years after a 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 the contact information at issue, in combination with email addresses, could be used for the purpose of phishing, increasing vulnerability to identity theft and fraud. Credentials may be used to compromise other online accounts. These are significant harms.

The likelihood of harm is increased because the personal information was compromised due to the malicious action (deliberate intrusion, deployment of malware and network penetration tools) of an unauthorized actor. Further, a lack of reported incidents does not mitigate against future harms, as phishing, identity theft, and fraud can happen months or years after a 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 affected individuals in emails dated October 1, and October 2, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner