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	Le Creuset Canada Inc. (Organization)
Decision number (file number)	P2021-ND-259 (File #021898)
Date notice received by OIPC	June 29, 2021
Date Organization last provided information	December 15, 2021
Date of decision	February 8, 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 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 headquartered in Montreal, Quebec 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: Online consumers: • name, • email address, • telephone number, • billing address, • shipping address, and • order information. Employees: • name, • address, • telephone number, • email address, • date of birth, • social insurance number, • employment history, • signature, • salary / payroll information, • vacation information,

	• tax information, • bank account information, • group insurance information, • RRSP information, • credit card information, • reference questionnaires (name of reference, feedback about candidate), • passport, • licence, • other identification card details, • CNESST file number, • medical note, and • bankruptcy letter. Individuals who made "Non-Website transactions": • name, • telephone number, • email address, and • credit card information. Individuals to whom orders placed by other individuals were shipped: • name, and • address. Employees who placed employee orders using a corporate email address: • name, • address, • telephone number, and • order information. Corporate wholesale customers: • credit card information, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 7, 2021, the Organization discovered it was the subject of a cyberattack when a malware alert was triggered. • An investigation determined that on or about June 4, 2021, a threat actor gained access to the Organization's network via legacy network appliances/services and compromised credentials. It is not known how the credentials were obtained. • The threat actor gained access to user accounts with elevated privileges through brute-force attack. • The incident was contained on or about June 11, 2021; however, the Organization detected additional attempts to access the network two days later on June 13, 2021. • The Organization assumes that the threat actor successfully exfiltrated records via FTP during the attack.
Affected individuals	The incident affected approximately 98,500 individuals, including 7,750 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Terminated the attacker's network access. • Blocked malicious IP addresses. • Adjusted firewall rules to block certain traffic. • Decommissioned legacy services and rebuilt potentially compromised services. • Reset all user account passwords and increased required password strength. • Tightened rulesets that govern network traffic. • Disabled some website functionality to limit potential misuse of personal information (e.g.: order lookup). • Offered credit monitoring and identity theft insurance to some affected individuals. • Offered to cover certain employees' out-of-pocket expenses incurred by the incident. • Implemented managed cybersecurity services. • Increased enforcement of multi-factor authentication. • Notified law enforcement. • Additional security and organizational changes under review, including the implementation of periodic risk assessments and penetration/vulnerability testing.
Steps taken to notify individuals of the incident	Most affected individuals were notified by Microsoft Teams and / or email between June 11 and June 30, 2021. The Organization also posted a public statement about the incident on June 30, 2021. The Organization also said "With respect to two consumers, the compromised information consisted of each consumer's name and complete credit card number. [The Organization] has no means of contacting these individuals and therefore direct notification was

	not possible." However, the Organization also reported "There is no reason to believe any of these individuals reside in Alberta", and: *In any event, however, these individuals will be informed of the incident through indirect notice, as a result of the public statement and frequently asked questions that will be posted to [the Organization's] Canadian website, and have therefore been advised of additional measures that they can take to minimize any risk of harm.*
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: *Employees whose social insurance numbers and other employment-related information was compromised as well as consumers who engaged in Non-Website Transactions whose full credit card numbers were compromised may be subject to a heightened risk of identity theft or fraud as a result of this incident.* *All individuals whose email addresses were compromised in connection with either their employment details or order information may be subject to phishing attacks.* The Organization also said the following with respect to potentially affected consumers who engaged in "Non-Website transactions": *... with respect to 22 of these 24 consumers, there does not appear to be a real risk of significant harm given the low sensitivity of the information compromised. Specifically:* • *With respect to 16 consumers, the potentially compromised information consisted of only each consumer's name and a partial credit card number (e.g., last four digits); and* • *With respect to six consumers, the potentially compromised information consisted of only each consumer's name, a partial credit card number, and a credit card expiration date. ...* The Organization also said: *With respect to recipients of online orders (approximately 350-370 of which appear to be in Alberta), the compromised information included only each individual's name and physical address. With respect to employees*

	who placed orders using the common... account whose information was not otherwise compromised (one of whom appears to be in Alberta), the compromised information included each individual's name, physical address, phone number, order number(s) and order date(s). *In [the Organization's] view, neither of these groups of individuals faces a real risk of significant harm given the low sensitivity of the personal information involved. Notably, the compromised information did not include email addresses, payment information, or other more sensitive employee data.* With respect to individuals who provided references for candidates for employment, the Organization said: *The forms do not include references' contact information. [The Organization] did not investigate whether it still has access to any contact information for the references and in any event would not have directly notified the references because there is no reason to believe that they face a real risk of significant harm.* In my view, a reasonable person would consider that the contact, identity (date of birth, social insurance number, passport, licence, other ID), employment (work history, salary), and financial (tax, banking, RRSP, credit card) information at issue could be used for the purposes of identity theft, fraud, negative affects on a credit record, or financial loss. The medical, bankruptcy, and candidate reference information could be used to cause the harms of embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing or spear phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms. I agree with the Organization's assessment that partial credit card numbers and the names of references could not be used to cause significant harm. I also agree that name, physical address, telephone number, order number(s) and order date(s) alone could not be used to cause 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 reported: *Although the attackers may have had malicious intent, based on their conduct while in [the Organization's] network, there is no reason to believe that they were specifically targeting individuals' personal information (as opposed to, for example, corporate records).* *Moreover, [the Organization's] investigation to date has not revealed the use of any compromised information for fraudulent purposes or the public disclosure of such information.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, exfiltration of records, attempted deployment of malware). The Organization can only speculate as to the attacker's motive, and the lack of reported misuse or public disclosure does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately 7 days before the unauthorized access was terminated. The threat actor also attempted to regain access to the network, suggesting that the environment was being actively exploited.

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, identity (date of birth, social insurance number, passport, licence, other ID), employment (work history, salary), and financial (tax, banking, RRSP, credit card) information at issue could be used for the purposes of identity theft, fraud, negative affects on a credit record, or financial loss. The medical, bankruptcy, and candidate reference information could be used to cause the harms of embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing or spear phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

I agree with the Organization's assessment that partial credit card numbers and the names of references could not be used to cause significant harm. I also agree that name, physical address, telephone number, order number(s) and order date(s) alone could not be used to cause significant harm.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, exfiltration of records, attempted deployment of malware). The Organization can only speculate as to the attacker's motive, and the lack of reported misuse or public disclosure does not mitigate against future harms as identity

theft, fraud, and phishing can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately 7 days before the unauthorized access was terminated. The threat actor also attempted to regain access to the network, suggesting that the environment was being actively exploited.

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 most of the affected individuals by Microsoft Teams and / or email between June 11 and June 30, 2021, in accordance with the Regulation. The Organization is not required to notify those affected individuals again.

The Organization also said "With respect to two consumers, the compromised information consisted of each consumer's name and complete credit card number. [The Organization] has no means of contacting these individuals and therefore direct notification was not possible." However, the Organization also reported "There is no reason to believe any of these individuals reside in Alberta", and noted that "these individuals will be informed of the incident through indirect notice, as a result of the public statement and frequently asked questions that will be posted to [the Organization's] Canadian website". The Organization posted a public statement about the incident on June 30, 2021.

Section 19.1(2) of the Regulation states that "the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given the Organization's submission, and in the circumstance where the Organization *does not* have contact information for an affected individual, indirect notice as provided by the Organization is reasonable.

Jill Clayton
Information and Privacy Commissioner