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	Tupperware U.S., Inc. (Organization)
Decision number (file number)	P2020-ND-068 (File # 015701)
Date notice received by OIPC	April 21, 2020
Date Organization last provided information	April 21, 2020
Date of decision	July 15, 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, • billing and shipping address, • telephone number, • email address, payment card number, expiry date, and card security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's websites Tupperware.com and Tupperware.ca.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 24, 2020, the Organization identified unauthorized code had been inserted into the code that runs its Tupperware U.S. and Tupperware Canada e-commerce websites, Tupperware.com and Tupperware.ca. • The Organization's investigation found the code was designed to capture information entered by customers during the checkout process on these websites. It was further determined the code was present on the websites from March 19, 2020 to March 24, 2020.
Affected individuals	The incident affected 4,763 individuals, including 168 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Removed the unauthorized code, launched an investigation, engaged a cybersecurity firm. • Notified law enforcement and payment card networks. • Provided affected individuals with additional steps that they can take to protect their information. • Implemented enhanced safeguards in order to further protect its systems.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on April 21, 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 "There is a potential that unauthorized parties could make fraudulent charges on the payment cards." In my view, a reasonable person would consider the financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.
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 "It is unlikely that harm will result from this incident, as the data involved is limited to payment card information, and the payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. In addition, the individual notice letters provide information on additional steps that individuals can take to protect their 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 an unknown third party. It appears the information was

	exposed for approximately 1 week. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. It appears the information was exposed for approximately 1 week. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 by letter on April 21, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner