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	Muji USA, Ltd. (Organization)
Decision number (file number)	P2017-ND-20 (File #001876)
Date notice received by OIPC	November 12, 2015
Date Organization last provided information	November 12, 2015
Date of decision	January 30, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates principally out of New York, NY, U.S.A. and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • address, • payment card number, • expiry date, • security code, and • purchase information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization received reports that some individuals had unauthorized charges made to their personal credit cards, suggesting that the Organization's on-line website may have been compromised. • The Organization closed its on-line web shop and retained cybersecurity specialists to investigate. • The Organization believes that an unauthorized third party used malicious software (malware) to infiltrate its on-line server and collect personal information. • The incident potentially affected individuals who made on-line purchases between January 22, 2015 and July 20, 2015.
Affected individuals	The incident affected 1,103 Canadians, including 104 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization removed the malware, increased its security, and suspended its e-commerce website. • Notified the Office of the Privacy Commissioner of Canada and other Canadian provinces. • Offered one year free credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	Written notice of the incident was mailed to affected residents of Alberta on November 16, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 assess the harm that might result from this incident, but reported that it was "in the process of alerting all individuals in Canada whose order information may have been accessed. This notification also will include information on how to seek help with identity theft in Canada." In my view, the information at issue could be used to cause the harms of 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 specifically assess the likelihood of harm resulting from this incident but reported that it would "provide potentially affected individuals means to obtain assistance from [the Organization] as well as information on how they can protect themselves from or address issues of fraud or identity theft. To further mitigate any risk of harm caused by this unexpected incident, [the Organization] will offer 1 year of credit monitoring…". In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the malware was operational for approximately 6 months. The Organization received reports of unauthorized credit card charges that led to an investigation and discovery of the incident.

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 as a result of this incident. The information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the malware was operational for approximately 6 months. The Organization received reports of unauthorized credit card charges that led to an investigation and discovery of the incident. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that written notice of the incident, in accordance with the Regulation, was mailed to affected residents of Alberta on November 16, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner