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	Rakuten Kobo Inc. (Organization)
Decision number (file number)	P2021-ND-122 (File #017845)
Date notice received by OIPC	October 22, 2020
Date Organization last provided information	April 6, 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 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, • telephone number, • date of birth, • gender, • address, and • last four digits of credit card. 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 June 17, 2021, the Organization was victim of a phishing attack when an employee opened a malicious email attachment. After the initial breach, the attackers installed additional tools to propagate their attack. • The incident was discovered 68 days later on August 24, 2020 when abnormal CPU utilization was detected on a database server. • For the following 5 days, the Organization analyzed the breach and eliminated the attackers' access, effective August 29, 2020. • The Organization's investigation determined that the attackers accessed and ran searches in a customer database.
Affected individuals	The incident affected 189 individuals, including 14 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated the incident with the assistance of forensic experts. • Contained the incident and removed the attackers' access. • Shut down and removed infected servers from production. • Implemented additional monitoring software to identify suspicious activity. • Reset all employee passwords. • Offered 24 months of identity theft and credit monitoring services to impacted individuals. • Training employees regarding phishing attacks. • Implemented two-factor authentication.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 20, 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 reports: "there is a potential risk of identity theft and a speculative risk of fraud for the individuals affected in Alberta." "The personal information of the individuals affected in Alberta involves name and date of birth and are of moderate sensitivity, as it is possible that such information could be used to conduct the specified harm noted above." I agree with the Organization's assessment. A reasonable person would consider the identity (date of birth), contact (address, telephone number) and financial information (last four digits of credit card) 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 reports: *[T]he likelihood that harm could result is moderate. While [the Organization] has no evidence that the personal information at issue has been misused by the external threat actors, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes of identity theft and fraud. The incident appears to have been caused by a known actor with malicious intent which may increase the possibility that harm could result. Credit Card data was limited to the last four digits of any potentially-valid cardholder number, and no other credit card data types were at risk. [The Organization] is of the view that the risk of fraud and financial loss is low, as a result.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the action of a known actor with malicious intent (phishing, deliberate intrusion). A lack of evidence of misuse to date does not mitigate against future harms, as identity theft and fraud can happen months or years after a breach. Further, the attackers had access to the Organization's network for approximately 70 days.

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 identity (date of birth), contact (address, telephone number) and financial information (last four digits of credit card) at issue could be used to cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the action of a known actor with malicious intent (phishing, deliberate intrusion). A lack of evidence of misuse to date does not mitigate against future harms, as identity theft and fraud can happen months or years after a breach. Further, the attackers had access to the Organization's network for approximately 70 days.

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 an email, dated October 20, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner