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	Shopper+ Inc. (Organization)
Decision number (file number)	P2023-ND-013 (File #029271)
Date notice received by OIPC	March 1, 2023
Date Organization last provided information	March 10, 2023
Date of decision	April 21, 2023
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 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: • name, • gender, • date of birth, • physical address, • telephone number, • email address, • customer ID, • date of first and last order, • frequency of orders, • total amount spent on orders, • "language settings (EN/FR)," • organization name, and/or • company name. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization operates a number of online storefronts. In the course of its operations, they obtain certain services from Amazon Web Services (AWS). • On February 8, 2023, the Organization "received feedback from an anonymous caller about a data file allegedly containing ... customer records leaked on a ... breach forum." • The Organization investigated; they assessed the records to be "highly similar to a CRM-exported data file with customer records stored on AWS S3."[1] • The Organization initially reported that the incident is the result of an insider threat or a "misconfiguration" of their AWS S3 environment, enabling the "enumeration ... and subsequent exfiltration" of data. • On March 7, 2023, the Organization clarified "the likeliest scenario is that the address of the AWS S3 object associated to the [data] ... was inadvertently exposed to the internet" between "September 14, 2020 ... and February 5, 2023." "A precise date cannot be determined because there is limited logging capability within the Organization's test environment, as is characteristic of such non-production environments." • The data file "was made available on the breach forums on February 5, 2023" and "is still available" as of March 7, 2023.
Affected individuals	The incident affected 874,276 "account holders" including 63,759 who "have an address in Alberta."
Steps taken to reduce risk of harm to individuals	• "Attempting to limit the availability of the Data File either directly through a deindexing request submitted to search engines." • Reviewed administrative and technical safeguards. • Updated processes and procedures, including access controls for operations involving customer data. • Implemented additional technical safeguards. • Notified the Canadian Centre for Cyber Security. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 10, 2023.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	

[1] Amazon Simple Storage Service.

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 the possible harms of "spam, fraud or successful phishing attempts, which may be further facilitated through order details." On March 7, 2023, the Organization added: *Affected individuals are namely at risk of successful phishing attempts, which may be further facilitated through the availability of order details and other available data points. Successful phishing can be leveraged to compromise credentials with the intent of causing financial or reputational harms to affected individuals.* I agree with the Organization's assessment. A reasonable person would consider that the identity (name, gender, date of birth), contact (email / physical address, telephone number), and customer information (customer ID, dates and frequency of orders, amount spent, name of organization or company) could be used for the purposes of phishing, increasing the affected individuals vulnerability to identity theft, fraud, and possibly the compromise of credentials. 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 reported: *[The Organization] does not believe the website making the Data File available, the website hosting the Data File or the user who made the post leaking the Data File will remove it.* *While the affected information is less sensitive in nature and there is no evidence that the Data File has been acquired by anyone other than the unauthorized posting, its mere presence on the "breach" forum is sufficient for [the Organization] to notify affected individuals about the potential consequences...* *The existence of the Data File is not broadly known at this time, as it is made available on a notorious breach forum associated with illegal activities.* On March 7, 2023, the Organization added: *The Organization's believes there is a real risk of significant harm to certain individuals where the information is more sensitive, for instance, where there is a real date of birth. Please note that the most "date of birth" fields are either blank or contain inaccurate data.* I accept the Organization's assessment. 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 threat actor (unauthorized access, exfiltration and publication of personal information). The information remains available for download from a "breach forum" and the Organization does not believe the data will be removed/recovered. The lack of evidence that personal information has been misused or further distributed does not mitigate against future harm; published personal information can be misused months or years after an 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.

The identity (name, gender, date of birth), contact (email / physical address, telephone number), and customer information (customer ID, dates and frequency of orders, amount spent, name of organization or company) could be used for the purposes of phishing, increasing the affected individuals vulnerability to identity theft, fraud, and possibly the compromise of credentials. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (unauthorized access, exfiltration and publication of personal information). The information remains available for download from a "breach forum" and the Organization does not believe the data will be removed/recovered. The lack of evidence that personal information has been misused or further distributed does not mitigate against future harm; published personal information can be misused months or years after an incident.

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 email on March 10, 2023. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance