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	PayPal Canada Co. (Organization)
Decision number (file number)	P2023-ND-011 (File #028445)
Date notice received by OIPC	December 23, 2022
Date Organization last provided information	January 4, 2023
Date of decision	February 17, 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 Toronto, ON, 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, • date of birth, • address, • telephone number, and • knowledge that credential combinations were valid. 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	• Between December 6 and 8, 2022, the Organization was subject to a credential stuffing attack. • An investigation confirmed personal information may have been accessed and downloaded by the unauthorized third party.

Affected individuals	The incident affected 107,053 individuals, 1,875 of whom are in Canada. Of those, 255 individuals' information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• "Masked the personal information so it is no longer visible." • Engaged external expertise to investigate the incident. • Reset passwords for affected accounts. • Implemented additional safeguards and dark web monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 2, 2023.
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: *1) Risk of identity theft given the exposure of personal data including date of birth. However, this risk is mitigated by the fact that the incident did not result in the compromise of any copies of identification documents or similar.* *2) Risk of unauthorised access to accounts for which the relevant individuals' re-used their … credentials given, after succesfully [sic] being used to authenticate into an individual's … account the unauthorized third party responsible for the incident may have attempted to use the credentials to access further accounts associated with the individual(s) in additional credential stuffing attacks. However, this risk is mitigated by [the Organization's] planned communication to individuals advising them to reset their passwords on any accounts for which they reused the password associated with their … account.* *3) Risk of targetted [sic] spearphishing attacks against individuals using the information obtained through the incident. This risk will be mitigated, however, by [the Organization] informing all potentially affected individuals about the incident.* I accept the Organization's assessment. A reasonable person would consider that name, date of birth, address, and telephone number could be used to cause the harms of identity theft, fraud, and possibly phishing. Knowledge that credential combinations were valid could be used to compromise other online accounts via credential stuffing. 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: *… believes that the risk of identity theft arising as a result of this incident is low given that further information would be needed in order to assume an individuals' identity (e.g., copy of official identity document).* *[the Organization] cannot exclude the risk of follow-on spearphishing attacks by the unauthorised third party that could cause harm to individuals. PayPal has not, however, identified any such attacks in practice. [The Organization] believes this to be a medium risk.* *…* *Note also though that: 1) The incident did not allow the unauthorized third party to make transactions using the individuals' … accounts; and 2) To date, [the Organization] has not identified any misuse or public dissemination of the personal data involved.* 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 unauthorized third party (credential stuffing attack, possible exfiltration of personal information). A lack of evidence that personal information has been misused or further disseminated does not mitigate against future harm, as identity theft, fraud, and phishing may occur 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.

Name, date of birth, address, and telephone number could be used to cause the harms of identity theft, fraud, and possibly phishing. Knowledge that credential combinations were valid could be used to compromise other online accounts via credential stuffing. 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 an unauthorized third party (credential stuffing attack, possible exfiltration of personal information). A lack of evidence that personal information has been misused or further disseminated does not mitigate against future harm, as identity theft, fraud, and phishing may occur 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 January 2, 2023, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance