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	Wealthsimple Inc. (Organization)
Decision number (file number)	P2021-ND-221 (File #020133)
Date notice received by OIPC	March 13, 2021
Date Organization last provided information	September 9, 2021
Date of decision	November 12, 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"	Wealthsimple Inc. provides customer facing online investment management (Wealthsimple Trade and Invest) and tax return filing services (Wealthsimple Tax). The Organization operates in Alberta 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: For one individual: • name, • telephone number, • email address, • residential address, • mailing address, • date of birth, • income, • deductions, • donations, • social insurance number, • tax return information, • valid credentials confirmed during attack, • password hint, • account settings, • user preference settings,

	• IP addresses, and • past login information. For two individuals: • first and /or last name, • email address, • valid credentials confirmed during attack, • password hint, • account settings, • user preference settings, • IP addresses, and • past login information. For twenty-eight individuals: • email address, • valid credentials confirmed during attack, • password hint, • account settings, • user preference settings, • IP addresses, and • past login information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 5, 2021, the Organization detected unauthorized access to user accounts. It reported the unauthorized access was the result of a credential-stuffing attack. • An investigation determined that the credentials were not obtained from the Organization's network. Instead, it is believed that the unauthorized actor obtained user account credentials from a third party. • Subsequently, individuals who re-used the same username and password combination for other services, as obtained by the attacker from the third party, were affected in the incident.
Affected individuals	The incident affected 31 individuals in Canada, including at least 1 whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	• Disabled affected accounts. • Investigated the incident. • Reviewed IP addresses associated with the attack in order to differentiate unauthorized and normal activity. • Blocked unauthorized traffic and temporarily restricted services to IPs located within certain jurisdictions. • Verified the status of security safeguards already in place. • Implemented additional safeguards such as suspending accounts accessed from known-bad IP addresses. • Encouraged users to not re-use passwords. • "Backfilling" mandatory two-factor authentication for clients and implemented requirement for users to use two-factor authentication. • Offered one year subscription to a password manager service. • Offered credit monitoring services to three affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 11, 2021.
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: *For the one Alberta confirmed resident whose information was accessed, this user completed, or partially completed, a tax return. The possible harms in this context include (1) the potential for identity theft or (2) phishing, because while the attacker already had the email address of the user, the attacker managed to confirm that the email address was connected to a valid ... account. ...* *For the thirty individuals whose jurisdiction is unknown, the potential harm is limited since once the accounts were accessed, only two individuals in this group of thirty provided additional personal information, which may have been in one case their first name, or in the other case, their first name and last name.* In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing, increasing the affected individuals' vulnerability to the above. Confirmed credentials, by virtue of a successful credential-stuffing attack, could be used to compromise other online accounts. 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 that it... *... is not aware of any actual use of the information that may have been accessed in connection with this incident.* *For the one confirmed Alberta resident whose tax return information was accessed, while identity theft or phishing are possibilities as outlined above, [the Organization] has no information that would enable it to assess the likelihood that harm will result due to this incident. [The Organization] consequently sought to mitigate the potential risk in this context by notifying the affected individual to enable them to be vigilant and by offering two years of complimentary credit monitoring.* *For the two individuals amongst the thirty whose jurisdiction is unknown and who had populated a first name or a first name and last name, the likelihood of harm resulting due to this incident appears remote given the limited personal information involved. The likelihood of harm resulting due to this incident for the remaining twenty eight (who had not even provided a name) is even more unlikely.* 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 a third party (credential-stuffing attack). The lack of reported misuse of the personal information does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach. The Organization's report of the breach is not clear as to how long the information may have been exposed.
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 that the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing, increasing the affected individuals' vulnerability to the above. Confirmed credentials, by virtue of a successful credential-stuffing attack, could be used to compromise other online accounts. 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 third party (credential-stuffing attack). The lack of reported misuse of the personal information does not mitigate against future harms as identity theft,	

fraud, and phishing can occur months or years after a breach. The Organization's report of the breach is not clear as to how long the information may have been exposed.

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 11, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner