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 Financial Corp. (Organization)
Decision number (file number)	P2021-ND-204 (File #017843)
Date notice received by OIPC	October 21, 2020
Date Organization last provided information	November 20, 2020
Date of decision	October 18, 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 the 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 some or all of the following information: <u>12 Individuals</u>: • email address, and • password. <u>11 Individuals</u>: • name, • postal address, • telephone number, • email address, • social insurance number, • relationship, • IP address, • password, • investment activity, • balances, • current employment status, • past logins, • account beneficiary, and • the name and email addresses of one (1) user's spouse.

	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 October 13, 2020, the Organization became aware of a credential stuffing incident involving suspicious attempts to access data from certain user accounts. • The unauthorized third party was able to log into client accounts between October 9, 2020, and October 13, 2020, using a valid email address and password. • The Organization's investigation discovered that passwords were not obtained from its systems. • The Organization believes that an unauthorized individual may have obtained client passwords from another site or app where clients used the same password as the one for their Organization account.
Affected individuals	The incident affected 23 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Manually reviewed the incident and suspicious IP addresses to isolate the suspicious attempts to access data from normal user activity and ensure the incident was contained. • Investigating to determine the cause and scope of the incident. • Disabled access to all user accounts involved to contain the incident. • Identified IPs participating in the attack and banning them permanently. • Offered a one (1) year complimentary subscription for a password manager service and two (2) years of complimentary credit monitoring services. • Notified data protection regulators. • Implementing new information security controls. • Encouraging users not to re-use passwords across different websites or apps to better protect their accounts. • Reminding users that a two-factor authentication option has been available and that it should be enabled to better protect their accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 21, 2020 and on November 16, 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 did not specifically identify the types of harms that might result fro this incident, but its letter and/or notification to affected individuals said: *Watch out for phishing emails: Be careful about any emails you receive asking for personal information. Always verify the identity of the requester. Most legitimate businesses will not require you to provide personal information (including usernames/passwords) via email.* 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 and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to 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 provide an assessment of the likelihood that significant harm will result from this incident, but the Organization did say: *Based on its investigation, the [Organization] has no evidence that personal information was exfiltrated by the threat actor."* In my view, a reasonable person would consider the risk of harm is increased as the incident was the result of a deliberate credential stuffing attack. The Organization reported that the unauthorized actor used the credentials and accessed users' accounts illegally and without authorization. The attacks appear to have been ongoing for approximately 4 days before the Organization discovered the threat.

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 and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The risk of harm is increased as the incident was the result of a deliberate credential stuffing attack. The Organization reported that the unauthorized actor used the credentials and accessed users' accounts illegally and without authorization. The attacks appear to have been ongoing for approximately 4 days before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose 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 letter on October 21, 2020 and on November 16, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner