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	SimpleTax Software Inc. (Organization)
Decision number (file number)	P2020-ND-186 (File #016338)
Date notice received by OIPC	July 6, 2020
Date Organization last provided information	July 6, 2020
Date of decision	December 16, 2020
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: **Group 1 (at least one profile associated with account was accessed)** • first and last name, • social insurance number, • date of birth, • residential/mailing address, • email address, • telephone number, • tax return data, 2010-2019 (e.g. income, deductions), • confirmation that valid user credentials matched account, • current password hint, • user preference settings, • last login times, • IP address, • list of account profiles, • list of tax returns prepared, and • status of tax return submissions.

	Group 2 (no profile associated with account was accessed) • confirmation that valid user credentials matched account, • current password hint, • user preference settings, • last login times, • IP address, • list of account profiles, • list of tax returns prepared, and • status of tax return submissions. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's tax return preparation platform.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 2, 2020, the Organization became aware of a credential stuffing incident involving attempts to access data from certain user accounts. • The Organization reported that it appears an unauthorized individual(s) was able to log in to user accounts between June 28 and July 2, 2020, using valid usernames and passwords. The Organization's investigation indicates that the credentials were not obtained from its systems, but rather from another site or app where the user used the same password. • The Organization's investigation was able to identify whether one or more profiles within an account were accessed, or may have been accessed. Based on the available logging data, however, the Organization cannot be sure in all cases which specific profile(s) within an account may have been accessed.
Affected individuals	The incident affected approximately 1,676 residents of Alberta (including 1,104 in Group 1, and 572 in Group 2).
Steps taken to reduce risk of harm to individuals	• Investigated to determine the cause and scope of the incident. • Disabled access to all user accounts. • Encouraged users not to re-use passwords across different websites or apps to better protect their accounts. • Reminded users that two-factor authentication is available. • Implemented a new web application firewall. • Enhanced monitoring of user accounts to detect additional suspicious activity.

	• Enhanced authentication procedures. • Reported incident to law enforcement. • Notified data protection authorities. • Offered complimentary credit monitoring arrangements for Group 1 individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 5, 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 reported, • "For Group 1, the personal information accessible to the unauthorized individual included sensitive personal information that could be used in the context of identity theft and phishing"; • "For Group 2, the personal information accessible to the unauthorized individual was much more limited, though the confirmation that a valid account existed—in combination with the email address that the unauthorized individual already had—could conceivably be used in a phishing attack." In my view, a reasonable person would consider 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 the purposes of phishing, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts and for phishing purposes. 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 would result from this incident. However, it reported that it is offering credit monitoring to Group 1 individuals, and is notifying both Group 1 and Group 2 individuals of the incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from malicious action by an unknown individual(s) (credential-stuffing). The Organization cannot be sure in all cases which specific profile(s) within an account may have been accessed in Group 1. Further, the information may have been exposed for approximately four (4) 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 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 the purposes of phishing, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts and for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because it resulted from malicious action by an unknown individual(s) (credential-stuffing). The Organization cannot be sure in all cases which specific profile(s) within an account may have been accessed in Group 1. Further, the information may have been exposed for approximately four (4) 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 by email on July 5, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner