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	Tamarack Psychology (Organization)
Decision number (file number)	P2021-ND-106 (File #017700)
Date notice received by OIPC	July 21, 2020
Date Organization last provided information	March 18, 2021
Date of decision	March 31, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a Registered Psychologist and sole proprietor of a private practice offering psychological services. 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: • name, • home address, • date of birth, • email address, • telephone number, • name of insurance provider, • insurance ID number and group member number for claiming benefits, • professional credentials, • credit card information, • information on scheduling of psychological services, • mental health symptoms and brief descriptions of reasons for seeking psychological services, • requests from individuals seeking counselling and psychological services for themselves or a family member, typically providing a brief summary (1-2 sentences) of their reasons for seeking services,

	• signed consent forms for counselling, • referrals to other mental health professionals, and • court order relating to provision of psychological services. 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	• On July 6, 2020, the Organization received a phishing email that appeared to be from its email and website provider. • The email identified that the Organization's credit card payment did not go through because the card may have changed or expired. The credit card had in fact recently expired. The email requested the Organization update its credit card information. • The Organization provided the new credit card and login information but did not realize password information was also disclosed. • On July 8, 2020, a third party attempted to login to the Organization's account using the correct password (obtained from the phishing scam) but the attempt was blocked by IT security. • Also on July 8, 2020, a third party successfully changed the email password. • The Organization changed its email password again and added 2-Step verification to secure its account.
Affected individuals	The incident affected 64 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals. • Enhanced computer security. • Changed passwords. • Upgrading software. • Changed policies on how personal information such as credit card information, date of birth, insurance information will be collected moving forward. • Reported to the Canadian Anti-Fraud Centre.
Steps taken to notify individuals of the incident	Affected individuals were notified between July 19, 2020 and the end of July 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 the possible harms that may occur as a result of the breach are: • *possible upset if their email or phone number is used to spam them.* • *possibility of fraud or theft for the individual who provided their credit card information.* • *possible identity theft for person who provided their home address.* • *possible identity theft for person who provided their date of birth and insurance ID number and group number for claiming benefits.* In my view, a reasonable person would consider that the contact, identity, and account information at issue could be used to cause the harms of fraud, identity theft and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The health/medical information could potentially be used to cause hurt, humiliation or embarrassment These are all 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 information was only exposed for 1-3 hours, however it is possible the hacker had time to save the data in that time. Given that I was targeted for my credit card, it appears likely this is a financially motivated crime.* *The risk of harm of identity theft or financial fraud is possible for the one individual who shared their credit card information with me by email; for the one individual who provided both their date of birth and insurance ID number and group number for claiming benefits; and for the family whose lawyer sent me a court order document regarding provision of psychological services which included the family's dates of birth and other identifying and sensitive information.* 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 an unknown third party (deliberate intrusion) who possibly saved the information at issue. Although the Organization reported "...it appears likely this is a financially motivated crime", I do not find this to be reassuring. The Organization can only speculate as to the motives of the thief.

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 account information at issue could be used to cause the harms of fraud, identity theft and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The health/medical information could potentially be used to cause hurt, humiliation or embarrassment These are all 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 unknown third party (deliberate intrusion) who possibly saved the information at issue. Although the Organization reported "...it appears likely this is a financially motivated crime", I do not find this to be reassuring. The Organization can only speculate as to the motives of the thief. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals between July 19, 2020 and the end of July 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner