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	Sherwood Consulting Services, Inc. (Organization)
Decision number (file number)	P2021-ND-139 (File #017438)
Date notice received by OIPC	April 6, 2020
Date Organization last provided information	May 4, 2020
Date of decision	May 25, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates a private psychology practice out of two offices, one in Calgary and one in Cochrane. 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, • address, • Alberta Health Care number, • telephone number, • emergency contact information, • occupation, • reason for coming to therapy, • email address, • notes on symptoms each individual was experiencing, • family history, • substance use history, • medical history, • suicidal risk information, • occupational history information, • relationship history information, • current functioning information, as well as one file containing supervision information, • goals in therapy, • how the individual was functioning, etc.

	• session dates and times, and • amount of payment that was made and whether or not a receipt was issued. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 21, 2020, a psychologist with the Organization discovered her residential garage had been broken into and a briefcase and other items were missing from her vehicle. • The brief case included paper client files. These have not been recovered to date. • A computer that was stolen was protected with facial recognition software and encryption.
Affected individuals	The incident affected 9 individuals.
Steps taken to reduce risk of harm to individuals	• Reported the theft to the local police service and filed a report. • Wiped the codes on the garage door. • No longer leaving client files in vehicle(s), and bringing them in the home. • In the process of moving the practice to a fully electronic practice with no paper files.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone between March 23, 2020 and March 27, 2020 and by letter on April 3, 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: - *Embarrassment, shame, humiliation* - *Identity Theft (personal health care numbers)* - *Damage to reputation or relationships* - *Email phishing or spear-phishing attacks* - *Blackmail (due to sensitive nature of information)* I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information at issue could be used to cause the significant 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. The medical information could be used to cause damage to reputation and relationships, embarrassment, hurt, humiliation, and stress. 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: *An assessment of the likelihood of harm resulting is difficult, because it is unknown who obtained the information and whether or not they were actually interested in the information or just the computer that was also located in the briefcase (same has facial recognition software and encryption software). While it is speculation, Calgary Police Service believe that the main reason for the break in was to steal the license plate on my vehicle, as same was taken and another (stolen) license plate was attached to the car in its place. Further support of this theory is that the license plate that was left on the car was from a stolen vehicle that matched the make, model and colour of my car. The CPS believe the briefcase was taken because it was locked and had the individuals been able to get into the briefcase and take the computer, the files would most likely have been left behind, however this is also speculation and the motives of the individuals that took the briefcase are unknown*. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the paper documents have not been recovered to date. Although the Organization reported it believes the documents were not the target of the theft, this is only speculation.

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 and identity information at issue could be used to cause the significant 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. The medical information could be used to cause damage to reputation and relationships, embarrassment, hurt, humiliation, and stress. These are all significant harms.

The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the paper documents have not been recovered to date. Although the Organization reported it believes the documents were not the target of the theft, this is only speculation.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by telephone between March 23, 2020 and March 27, 2020 and by letter on April 3, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner