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	Troy Janzen Psychological Services (Organization)
Decision number (file number)	P2018-ND-139 (File #009361)
Date notice received by OIPC	August 10, 2018 (updated October 2, 2018)
Date Organization last provided information	October 18, 2018
Date of decision	October 30, 2018
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 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, • computer generated test scores, and • full psychological reports. 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	• The Organization is a sole practitioner psychologist. On June 29, 2018, a password protected laptop computer was stolen from a vehicle outside his home. The laptop was protected by a password but the hard drive was not encrypted.

	• The laptop contained a desktop Dropbox application on which various electronic client files were stored, some of which were protected using Microsoft Word's "encrypt with password" feature. Some files were PDF documents and were not further encrypted or password protected. • The Organization reported that Dropbox requires a password to access the online version of the application. The version of the Dropbox application on the laptop, however, was a downloaded version that did not require an additional password to access the files and folders once access to the hard drive was obtained. • The Organization cannot be certain that any of the MS Word or PDF files were actually available within the Dropbox application that had been downloaded to the laptop; the Organization is only surmising this from knowledge that the downloaded version of the application sometimes automatically syncs with the Dropbox account when a computer is connected to the internet. • The breach was discovered on June 29, 2018. The laptop has not been recovered.
Affected individuals	The incident affected approximately 372 individuals.
Steps taken to reduce risk of harm to individuals	• Delinked the Dropbox from the account such that it would not be possible to access the Dropbox account from the laptop. • Deleted all files from the Dropbox account after extracting and securely storing the files on an encrypted flash drive that has been secured. • Notified the Ministry of Children Services and will be providing a list describing the PDF files with names to begin notification on August 31, 2018. • Notified the principal at the school. • Notified the police. • Notified the Organization's regulatory body.
Steps taken to notify individuals of the incident	Six affected clients of the Organization were notified by telephone on September 25 and September 26, 2018. The parents of two affected students who were provided references by the Organization were notified by telephone on September 26, 2018 and October 3, 2018. Two affected individuals were clients via a contract with a school. The Organization reported the incident to the principal of the school on September 25, 2018. These client records would be subject to Alberta's *Freedom of Information and Protection of Privacy Act.*

	Some of the affected individuals were clients of Alberta Children's Services. The Organization reported the incident to the ministry on August 29, 2018. Children's Services requested a spreadsheet identifying affected clients so that it could notify them of the breach. These client records would be subject to Albert's *Freedom of Information and Protection of Privacy Act.* The Organization has not, to date, notified clients whose information is contained within the files protected by Microsoft Word's "encrypt with password" feature.
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 main concern would be humiliation and damage to reputation if the PDF files were accessed and reviewed or made public (we assume the potential for access to the password protected MS Word files is very low and as such, any attendant risk would be low to non-existant [sic]). For some of the PDF files which contained specific identifying information, it is possible that there is a risk of identity theft. As noted, access to the files was not the motivation for the theft, such that the risk of actual access to the files appears low." Further, "In most cases addresses and financial information were not included within the client files such that there is a low risk of identity theft." In my view, the identity information along with the medical information could be used to cause the harms of humiliation and damage to reputation. If addresses and financial information were involved, this information could be used to cause the harms of identity theft or 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 reported that "The information was contained on a password protected laptop within a Dropbox application. The majority of the files were further password protected, such that the risk of access to the patient files appears low. To date the information has not recovered. … There is no evidence of malicious intent or purpose. It is suspected that the motivation for the theft was to obtain items for resale for cash, in which case the theives [sic] would be likely to wipe the laptop harddrive [sic] for resale. The theives [sic] were identified to be a group of young persons but could not be specifically identified by eyewitnesses; accordingly, the prospects for recovery of the laptop appear low." In my view, a reasonable person would consider the likelihood of harm resulting from this incident to be increased because the personal information was compromised due to the malicious action of an unknown third part(ies) (theft). The Organization can only speculate on the thief's motives for stealing the laptop and its contents. Although the laptop containing the Dropbox application

	was password protected, and the MS Word documents within the Dropbox application were "encrypted with a password", the laptop's hard drive was not encrypted making the personal information in Dropbox vulnerable to unauthorized access.

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 affected individuals.

The identity information along with the medical information could be used to cause the harms of humiliation and damage to reputation. If addresses and financial information were involved, this information could be used to cause the harms of identity theft or fraud. 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 an unknown third part(ies) (theft). The Organization can only speculate on the thief's motives for stealing the laptop and its contents. Although the laptop containing the Dropbox application was password protected, and the MS Word documents within the Dropbox application were "encrypted with a password", the laptop's hard drive was not encrypted making the personal information in Dropbox vulnerable to unauthorized access.

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 whose personal information was not encrypted by telephone on September 25, 2018, September 26, 2018 and October 3, 2018 in accordance with the Regulation.

I further understand that two affected individuals were clients via a contract with a school and the Organization reported the incident to the principal of the school on September 25, 2018. Some of the affected individuals were clients of Alberta Children's Services and the Organization reported the incident to the ministry on August 29, 2018.

The Organization is required to notify the remaining individuals whose information was "encrypted with a password", in accordance with section 19.1 of the Regulation, and confirm to my office within ten (10) days of the date of this decision, that it has done so.

Jill Clayton
Information and Privacy Commissioner