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	Modern Solutions Counselling Services Ltd. (Organization)
Decision number (file number)	P2021-ND-268 (File #020895)
Date notice received by OIPC	February 5, 2021
Date Organization last provided information	February 5, 2021
Date of decision	February 9, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify these 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 psychotherapy clinic in Calgary, Alberta, and has a team of registered psychologists and registered clinical social workers who provide psychological assessment, counselling and consultation services. The reports containing the personal information at issue were the property of Canada Life Assurance Company ("Canada Life"). 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 found in paper receipts and on a laptop: • full name, • general description of services provided by the Organization (e.g. rehabilitation, medical coordination, or case management), • employer policy number with Canada Life, and • employee number, • Canada Life internal identification number, • employer name, • employment position, • medical diagnosis, • name of psychiatrist, and

	• past and present personal health information (including mental health history, current mental health difficulties, treatment plan, outcomes of treatment, recommendations for further treatment). 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 January 11, 2021, an unknown individual(s) broke into the Organization's office. • The perpetrators stole a laptop that contained medical reports regarding 19 identifiable individuals. The laptop was password protected but not encrypted. • There is no indication that the perpetrators have been able to access the information on the laptop. • The perpetrators also stole an unknown number of cheque receipts related to services the Organization provided to individuals insured by Canada Life. • It is believed the perpetrators were looking for cash or items of value that could be sold or traded for cash.
Affected individuals	The incident affected 85 individuals.
Steps taken to reduce risk of harm to individuals	• Notified Canada Life, law enforcement and the College of Alberta Psychologists (CAP) of the breach. • Contacted Microsoft who advised that the laptop would completely lock such the device will be totally inaccessible if the laptop ever connects to the internet again; however, Microsoft was not able to wipe the laptop remotely. • Enhanced security of the property. • Confirmed with all clinic therapists that laptops are: password protected, encrypted, and have a two step-verification process. • Personal information will no longer be stored on any laptops. • Purchasing a new higher security, locking filing cabinet that will be stored in a locked room within its premises.
Steps taken to notify individuals of the incident	The affected individuals were notified by email and by letter on February 5, 2021.

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 harm may include humiliation, embarrassment (sic), damage to reputation or relationships, loss of professional opportunities, identity theft.* 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. Medical information could be used to cause the significant harms of hurt, humiliation, or embarrassment.
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 it "…believes the risk that harm will result is very low, but ultimately still a "real risk"." The Organization said: *There is no evidence or information to suggest that the perpetrators have the technological sophistication to bypass the laptop's password. As a result, the risk of access to the reports contained therein is considered low, but still "real". There is also nothing to suggest that the perpetrators specifically targeted personal information.* *With respect to the receipts, only the individual's name and a description of services are readily understandable. The other information (employer policy number with Canada Life and employee number) is not identified as such and therefore without further information, no one would know what these numbers correspond to. Thus, the risk of harm resulting from unauthorized access/disclosure of the information on the receipts is also consider low, but still "real".* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization reported, "There is no evidence or information to suggest that the perpetrators have the technological sophistication to bypass the laptop's password" and "There is also nothing to suggest that the perpetrators specifically targeted personal information", I do not find this to be reassuring. The Organization can only speculate as to the technical expertise or the motives of the unknown perpetrator(s). The laptop was not encrypted and has not been recovered.

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. Medical information could be used to cause the significant harms of hurt, humiliation, or embarrassment. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization reported, "There is no evidence or information to suggest that the perpetrators have the technological sophistication to bypass the laptop's password" and "There is also nothing to suggest that the perpetrators specifically targeted personal information", I do not find this to be reassuring. The Organization can only speculate as to the technical expertise or the motives of the unknown perpetrator(s). The laptop was not encrypted and has not been recovered. 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 email or by letter on February 5, 2021. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner