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	C.L.C. Donald Wellness Group o/a Forward Psychology and Wellness Group (Organization)
Decision number (file number)	P2019-ND-097 (File #011704)
Date notice received by OIPC	January 14, 2019
Date Organization last provided information	February 7, 2019
Date of decision	July 15, 2019
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved: *For 33 clients or former clients: contact information (email addresses, names, and telephone numbers); information relating to client appointment scheduling; information relating to client treatment and psychological services offered by the organization.* *For 2 clients: contact information (email addresses, names, and telephone numbers); information relating to client appointment scheduling; information relating to client treatment and psychological services offered by the organization; financial information (void cheque and electronic fund transfer information).* *For 26 individuals who had inquired about … services but did not become clients: contact information (email addresses, names, and telephone numbers); some of these individuals included a brief description outlining their reasons for seeking support.*

	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 or around November 23, 2018, a laptop computer and other items were stolen from a vehicle belonging to the owner of the organization. • The laptop was password protected; there was no encryption or other security measures. • An email account was accessible via the laptop and did not require a password in order to gain access. The email account contained communications with the information at issue. • The Organization initially reported that it believed the thieves had accessed the laptop and email account and forwarded an email transfer of funds to an unauthorized account, successfully diverting funds. • The Organization subsequently reported that it believes a personal chequebook was stolen and the thieves attempted to open bank accounts, sometimes successfully. However, "There is no evidence that any of the personal information of clients or other individuals who inquired about services has been affected by these activities." • On December 4, 2018, the Edmonton Police Department was able to recover some items that were stolen, including a void cheque from a client of the organization. The laptop computer was not recovered.
Affected individuals	The incident affected 61 individuals.
Steps taken to reduce risk of harm to individuals	• Reported incident to law enforcement, insurance, and regulatory associations. • Changed passwords on all affected accounts and immediately ceased using the compromised email account. • Enhanced security of the laptop computer. • Changed the process for depositing electronic transfers. • Introduced encrypted USB drives to store client information.
Steps taken to notify individuals of the incident	The Organization reported that all affected individuals were notified by email and/or telephone by January 17, 2019.

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 possible harms include "Contact and identity information along with financial information poses a risk of harm associated with identity theft, fraud, and financial loss. Information that discloses that an individual has engaged or has sought to engage the services of a psychologist poses a risk of harm to the individual in that it could result in hurt and humiliation." I agree with the Organization's assessment. A reasonable person would consider that the contact, financial, and health/medical information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 "Increased risk of harm due to the nature of services involved, namely, psychological treatment services. It is unknown how many persons the information was exposed to. Increased risk of harm due to the malicious intent of the thieves. Increased risk of harm due to knowledge that the thieves accessed organization's email account and forwarded an electronic transfer from a client to themselves." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the breach resulted from malicious action (theft). The laptop was not encrypted and the email account with personal information was accessible without a password. The laptop 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, financial, and health/medical information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the breach resulted from malicious action (theft). The laptop was not encrypted and the email account with personal information was accessible without a password. The laptop 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 that all affected individuals were notified by email and/or telephone by January 17, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner