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	Lighthouse Psychological (Organization)
Decision number (file number)	P2023-ND-002 (File #023380)
Date notice received by OIPC	October 8, 2021
Date Organization last provided information	November 26, 2022
Date of decision	February 1, 2023
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 in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • email address. 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 August 8, 2021, the Organization sent an email to multiple email addresses using the "To" field instead of the "Bcc" field. • When the email went out all the people included in the email could see everyone else's email. • The email contained a notice that the psychologist's email had changed. • Two clients informed the Organization of the mistake.
Affected individuals	The incident affected 18 individuals.

Steps taken to reduce risk of harm to individuals	• No mass emails will be sent without having someone check that the email is bcc'd correctly.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on August 9, 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, *All of the individuals on the list would know that they had all contacted someone at Lighthouse Psychological either for information or for a session.* In my view, a reasonable person would consider that the information at issue (email address associated with a notice to clients of the Organization) could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and 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, *It is very unlikely that other people on the list would scrutinize the list since they would have no reason to contact those other people.* In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error. The unintended recipients are known to the Organization, two recipients reported the breach to the Organization. Despite this, however, it is not clear from the Organization's report of the incident whether the recipients were requested to delete the email and not forward or otherwise use or distribute it; further, it is not clear whether there are likely to be personal/professional relationships between the recipients such that hurt, humiliation and embarrassment might result.
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. The information at issue (email address associated with a notice to clients of the Organization) could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.	

The likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error. The unintended recipients are known to the Organization, two recipients reported the breach to the Organization. Despite this, however, it is not clear from the Organization's report of the incident whether the recipients were requested to delete the email and not forward or otherwise use or distribute it; further, it is not clear whether there are likely to be personal/professional relationships between the recipients such that hurt, humiliation and embarrassment might result.

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 Organization notified the affected individuals by email on August 9, 2021. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance