



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	The Ferrance Group (Organization)
Decision number (file number)	P2021-ND-255 (File #021098)
Date notice received by OIPC	March 16, 2021
Date Organization last provided information	November 25, 2021
Date of decision	December 10, 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 <i>Personal Information Protection Act</i> (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 an email containing a notice for online sessions that was sent to multiple email addresses using the “To” field instead of the “Bcc” field. This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">On March 12, 2021, an employee with the Organization inadvertently sent an email containing a notice for online sessions to multiple email addresses using the “To” field instead of the “Bcc” field.The breach was discovered on March 13, 2021, when one of the recipients reported the error to the Organization.
Affected individuals	The incident affected 27 individuals.

<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • Asked all affected individuals to delete the email. • Sent a substitute email. • Instituted a change in policies and procedures for administrative staff. • Using a different email platform.
<p>Steps taken to notify individuals of the incident</p>	<p>The affected individuals were notified by email on March 15, 2021.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<p>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.</p>	<p>The Organization reported,</p> <p style="text-align: center;"><i>Individuals may be identified as fellow clients of mine (a psychologist) to other clients mine through their email addresses.</i></p> <p>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.</p>
<p>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.</p>	<p>The Organization reported,</p> <p style="text-align: center;"><i>Although client privacy & confidentiality is of utmost importance, the possibility of being identified as a client was only available to fellow clients. It is very unlikely that people having similar circumstances and being being (sic) engaged in the same service would use identifying information against one another.</i></p> <p>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, one recipient reported the breach and the Organization requested that the recipients delete the email. Despite this, however, it is not clear from the Organization’s report of the incident whether the recipients confirmed deleting the email and not forwarding or otherwise using or distributing 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.</p>

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 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, one recipient reported the breach and the Organization requested that the recipients delete the email. Despite this, however, it is not clear from the Organization's report of the incident whether the recipients confirmed deleting the email and not forwarding or otherwise using or distributing 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 March 15, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner