



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Dorward & Company LLP Chartered Accountants (Organization)
Decision number (file number)	P2017-ND-88 (File #005906)
Date notice received by OIPC	June 22, 2017
Date Organization last provided information	June 22, 2017
Date of decision	July 10, 2017
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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• Social Insurance Number, and• total income for 2013-2016 tax years. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
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 June 16, 2017, an email was sent to an incorrect email address. There were 5 attachments to the emails, which contained signature pages for electronic filings for a client and his wife.• The incident was discovered on June 19, 2017 when the client contacted the Organization to question why he had not received the email.

	<ul style="list-style-type: none"> • The email was not encrypted, nor password protected. • The Organization emailed the incorrect address to advise of the error and to ask that the documents be deleted and for confirmation of same. To date, the Organization has not received a response.
Affected individuals	The incident affected two (2) Alberta residents.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Sent an email to incorrect address to advise of the error and to ask that the documents be deleted and for confirmation of same. • Working with IT provider to implement secure portal.
Steps taken to notify individuals of the incident	The Organization notified the affected individuals verbally on June 21, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<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 that “This could lead to identity theft which may result in fraud, financial loss or negative effects on a credit record.”</p> <p>I agree with the Organization. The identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss, and negative effects on a credit record.</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 that “the chance of harm occurring is low” but noted “An undeliverable notice was not received after sending the email and attachments, which leads us to believe the email address is active.”</p> <p>Despite the fact the incident did not result from malicious intent but rather human error, I have decided there is a real risk of harm in this case. The Organization believes the email address is active; however, the unintended recipient did not contact the Organization to report the error and has not responded to the Organization’s efforts to confirm the information has been deleted and not further disseminated.</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.	

The identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss, and negative effects on a credit record. Despite the fact the incident did not result from malicious intent but rather human error, the Organization believes the email address is active and the unintended recipient did not contact the Organization to report the error and has not responded to the Organization's efforts to confirm the information has been deleted and not further disseminated.

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 verbally on June 21, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner