



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	World Financial Group Insurance Agency of Canada Inc. (Organization)
Decision number (file number)	P2018-ND-110 (File #009395)
Date notice received by OIPC	August 9, 2018
Date Organization last provided information	August 9, 2018
Date of decision	August 13, 2018
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 whose information was collected in Alberta 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”	<p>The information at issue includes:</p> <ul style="list-style-type: none">• social insurance number,• address,• date of birth,• name,• telephone number,• email address,• Know Your Client form (KYC),• bank account information,• driver's license information,• RESP account documents and some general account information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.</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 May 30, 2018, an agent of the Organization sent email correspondence to a client's personal email address as well as an unknown party who had a very similar email address. This email correspondence included the information at issue, which was being sent to the client for record keeping purposes. On May 31, 2018, the unknown party reported the error to the Organization.
Affected individuals	The Organization reported the incident affected "Two (2) individuals."
Steps taken to reduce risk of harm to individuals	The Organization reported that "The client has been contacted and advised to access the below link, which outline measures to take in protecting against identity theft" (the link was to the Alberta OIPC website).
Steps taken to notify individuals of the incident	The Organization said it "...will be sending the client a written letter informing him about the recommended ... privacy breach cautionary steps and procedures."
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.	<p>The Organization reported that "Personal information may be misused" and also "Mid-level of sensitivity, as the client's SIN, DOB, PAD information, PR Card number, and Drivers license number were included."</p> <p>In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes. These are all significant harms.</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>The Organization reported that "The Probability that any harm will occur as a result of the incident is unknown, as it does appear that the error may have occurred with the email service used by the recipient." The Organization also said "This risk is somewhat mitigated as no copies of the original documents have been included" and "There has been no reported harm to client at this time."</p> <p>In my view, the likelihood of harm resulting from this breach is reduced because the incident was the result of human error and not malicious intent, and the unintended recipient reported the breach to the Organization. However, the Organization did not report any efforts to confirm that the unintended recipient would not use or further disclose the information, or that the information was deleted by the unintended recipient.</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 contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes. These are all significant harms. The likelihood of harm resulting from this breach is reduced because the incident was the result of human error and not malicious intent, and the unintended recipient reported the breach to the Organization. However, the Organization did not report any efforts to confirm that the unintended recipient would not use or further disclose the information, or that the information was deleted by the unintended recipient.

I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization contacted the affected individual and “intends to send a written letter”. **I require the Organization to confirm to my office in writing within 10 days of the date of this decision that it has notified the affected individuals in Alberta, in compliance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner